

Cyber Vision 2025

Cyber Vision 2025

**United States Air Force
Cyberspace
Science and Technology
Vision
2012-2025**



**AF/ST TR 12-01
13 December 2012**

Distribution A. Approved for public release; distribution is unlimited.
SAF/PA Public Release Case No. 2012-0439/460/715



U.S. AIR FORCE



Office of the
USAF Chief Scientist

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS OF THE AIR FORCE
WASHINGTON DC

17 January 2013

FROM: AF/ST

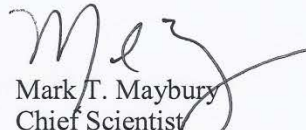
MEMORANDUM FOR ALMAJCOM-FOA-DRU/CC

SUBJECT: Cyber Vision 2025: Air Force Cyberspace Science & Technology Vision

Cyberspace is essential to all Air Force missions. Our *Core Function Master Plan for Cyberspace Superiority* articulates cyberspace as a domain in which, from which, and through which USAF missions are performed. Without well informed strategic choices, previously enduring sources of USAF advantage are at risk given an increasingly contested cyberspace environment. With careful investments and wise prioritization we can instead exploit new opportunities that ensure our sustained advantage.

Spearheaded by the Office of the Air Force Chief Scientist, *Cyber Vision 2025* was created in close collaboration with operational and technical experts from across the Air Force as well as the Nation. *Cyber Vision 2025* outlines our vision for the science and technology, acquisition, and operations needed to provide the assured cyberspace advantage to the Air Force, Combatant Commanders and interagency partners.

Air Force leaders at all levels are encouraged to become familiar with this vision and strategy and allow it to inform their daily decision making processes. Together, we will work to ensure that cyberspace empowers our Air Force to remain the world's most capable air, space, and cyberspace force.


Mark T. Maybury
Chief Scientist
United States Air Force

Executive Summary

Cyberspace is essential to all Air Force (AF) missions. It is a domain in which, from which, and through which AF operations are performed. Actions in cyberspace can have digital, kinetic, and human effects. Increasingly, the cyberspace domain is contested and/or denied. Yet our ability to address opportunities and threats is constrained by time, treasure, and talent.

Cyber Vision 2025 provides the Air Force vision and blueprint for cyber Science and Technology (S&T) spanning cyberspace, air, space, command and control, intelligence, and mission support. *Cyber Vision* focuses on S&T in the near (FY12-15), mid (FY16-20), and far (FY21-25) term, delineating where the Air Force should lead, follow, or watch. The Air Force Chief Scientist led the creation of *Cyber Vision 2025* in close collaboration with operational and technical experts from across the Air Force as well as the Nation (see Appendices C, D).

Cyber Vision 2025 finds that our missions are at risk from malicious insiders, insecure supply chains, and increasingly sophisticated adversaries as well as growing (often cyber) systems interdependencies. Fortunately, cyberspace S&T can provide assurance, resilience, affordability, and empowerment. However, this requires integration across authorities and domains, shaping of doctrine, policy, people, and processes, and intelligent partnering.

Motivated by a set of enduring cyberspace principles, *Cyber Vision 2025* recommends addressing these challenges by assuring and empowering missions. It recommends enhancing mission system security standards, making more effective use of authorities (e.g., Title 10/50/32), synchronizing multi-domain effects, and increasing the cost of adversary cyberspace operations. It also recommends improving cyber accessions and education and developing Air Force Cyberspace Elite (ACE) forces. It recommends requiring and designing-in security and securing weapon systems throughout their full life cycle. It recommends rapid, open, and iterative acquisition that engages user and test communities early. It recommends integrating cyber across all core functions, advancing partnerships, aligning funding, and orchestrating effort and effects across domains. *Cyber Vision 2025* recommends complexity reduction to ease verification and reduce life cycle cost, the development of trusted and self-healing networks and information, the creation of agile, resilient, disaggregated mission architectures, and the advancement of real-time cyber situational awareness/prediction and cyber S&T intelligence. Across all Air Force domains of operation, *Cyber Vision 2025* recommends science and technology to improve foundations of trust, enhance human machine interactions, enhance agility and resilience, and assure and empower missions, in collaboration with our partners.

Extracting value from *Cyber Vision 2025* will require adoption and sustained effort across the S&T, acquisition, and operational communities. May *Cyber Vision 2025* inspire you to advance the Air Force's assured cyber advantage to ensure the Air Force's ability to fly, flight, and win in air, space, and cyberspace.

Table of Contents

Executive Summaryiv
Table of Contentsv
Table of Figuresviii
List of Tablesviii

1. Introduction..... 1
 1.1 Motivation..... 1
 1.2 Vision and Alignment..... 1
 1.3 Methodology..... 3
 1.4 Enduring Principles..... 4
 1.5 S&T Partnerships 5
 1.6 S&T Roles: Lead, Follow, Watch..... 7
 1.7 Strategic Focus..... 7
 1.8 Significant Past Progress 7
 1.9 Cyber Vision 2025 Integrating Themes and Desired Outcomes 8
 1.9.1 Mission Assurance and Empowerment..... 8
 1.9.2 Agility and Resilience..... 8
 1.9.3 Optimized Human-Machine Systems 9
 1.9.4 Foundations of Trust 9
 1.9.5 Overarching Cyberspace S&T Desired Outcomes and Recommendations 9
 1.10 Structure of Cyber Vision 2025 Document 10

2. Future Environment and Cyberspace Threat 12
 2.1 Demographics, Economy, and Adversaries - 2025..... 12
 2.2 Technological Change - 2025 13
 2.3 Impacts..... 16
 2.4 Cyber Threats to Air Force Missions..... 16
 2.4.1 Threat Vectors..... 17
 2.4.2 Areas of Concern: Threat Increase and Attack Surface Expansion 19
 2.4.3 Cyber Operations (CO) Actors in 2025 - Refer to classified Annex. 20
 2.4.4 Threat Recommendations 20

3. Cyberspace..... 21
 3.1 Cyber Domain Strategic Context..... 21
 3.2 Findings and Recommendations 23
 3.2.1 Broaden Limited Cyber Mindset 23
 3.2.2 Enhance Situational Awareness & Understanding 24
 3.2.3 Assure Missions and Protect Critical Information in Fragile Architectures 24
 3.2.4 Create Hardened, Trusted, Self-Healing Networks & Cyber Physical Systems..... 25
 3.2.5 Develop Integrated and Full Spectrum Effects 25
 3.3 Cyber S&T Technologies 25
 3.3.1 Assure and Empower Missions..... 25
 3.3.2 Agile Operations and Resilient Defense 26
 3.3.3 Optimize Human-Machine Systems 27
 3.3.4 Trusted Foundations..... 28

- 4. Air Domain28
 - 4.1 Air Domain Strategic Context29
 - 4.2. Findings and Recommendations29
 - 4.2.1 Design-in Security to Address Insufficient Intelligence29
 - 4.2.2 Reduce Complexity and Enable Verification.....30
 - 4.2.3 Secure Full Life Cycle to Overcome Insufficient Security Architectures31
 - 4.2.4 Secure Platform Information Technology (IT)31
 - 4.2.5 Secure Command and Control (C2) Architecture to Address Brittleness32
 - 4.2.6 Overcome Insufficient Cyberspace Situational Awareness32
 - 4.3 Science and Technology Solutions32
 - 4.3.1 Anti-Tamper Root-of-Trust (L)33
 - 4.3.2 Cyber Black Box (L).....34
 - 4.3.3 Secure Maintenance Aids (L)34
 - 4.3.4 GPS Hardening and Alternatives (L).....33
 - 4.3.5 Collaborative/Cooperative Control (L).....33
 - 4.3.6 Advanced Satellite Communications (L).....34
 - 4.3.7 Managed Information Objects (L)35
 - 4.3.8 Trusted Cloud Computing (L)35
 - 4.3.9 Mission Mapping (L)35
 - 4.3.10 5th to 5th Platform Communications (L).....35
 - 4.4 Conclusions of Air Domain35
- 5. Space36
 - 5.1 Space Domain Strategic Context36
 - 5.2 Findings and Recommendations37
 - 5.2.1 Develop a Resilient Architecture to Address Space Network Vulnerabilities.....37
 - 5.2.2 Enhance Space Anomaly Detection and Attack Attribution.....39
 - 5.3 Space S&T Recommendations39
 - 5.3.1 Near Term: Cyber Test Beds, Space Sensors, Reconfigurable Antennas, Foundries.40
 - 5.3.2 Mid Term: Survivable Command, Control and Communications (C3), Malware Detection, Autonomous Self-healing Systems, Trusted Architectures41
 - 5.3.3 Far Term: Verified Code Generation, Intent Detection, Cognitive Communications, Space Quantum Key Distribution42
- 6. C2 and ISR42
 - 6.1 C2 and ISR Domain Strategic Context42
 - 6.2 Findings and Recommendations43
 - 6.2.1 Focus Teams of Experts to Assure Contested C2 and Intelligence, Surveillance, and Reconnaissance (ISR)43
 - 6.2.2 Create Intelligent Processing Capability to Overcome Massive Data Deluge44
 - 6.2.3 Assure Information Integrity of Cyber-enabled C2 and ISR at the Tactical Edge45
 - 6.2.4 Mature Cross Domain Synchronization.....46
 - 6.4 C2 and ISR S&T46
 - 6.4.1 Assure and Empower the Mission46
 - 6.4.2 Optimize Human-Machine Systems48
 - 6.4.3 Resilience and Agility49
 - 6.4.4 Foundations of Trust51
 - 6.5 Conclusion52

- 7. Enabling Science and Technology.....52
 - 7.1 Technology Area Overview.....52
 - 7.1.1 Foundations.....52
 - 7.1.2 Agility and Resilience.....52
 - 7.1.3 Human/Social/Machine Systems53
 - 7.1.4 Mission Assurance and Empowerment.....53
 - 7.2 Enabling Technology Examples54
 - 7.2.1 Foundations.....54
 - 7.2.2 Agility and Resilience.....54
 - 7.2.3 Human/Social/Machine Systems Enabling Technology.....55
 - 7.2.4 Mission Assurance and Empowerment Enabling Technology56
 - 7.3 Air Force Research: Near, Mid, and Far Term57
 - 7.3.1 Foundations.....57
 - 7.3.2 Agility and Resilience.....57
 - 7.3.3 Human/Social/Machine Systems58
 - 7.3.4 Mission Assurance and Empowerment.....58
- 8. Mission Support.....59
 - 8.1 Cyber Acquisition59
 - 8.1.1 Acquisition of Cyber Systems59
 - 8.1.2 Acquisition of Cyber-physical Systems.....60
 - 8.1.3 Cyber and Cyber-physical System Requirements.....61
 - 8.1.4 Cyber Assessment and Vulnerability Evaluations62
 - 8.1.5 Cyber Acquisition Recommendations63
 - 8.2 Test and Evaluation63
 - 8.2.1 Certification and Accreditation Shortfalls64
 - 8.2.2 Test and Evaluation Infrastructure.....64
 - 8.2.3 Test and Evaluation Recommendations.....65
 - 8.3 Education and Training.....65
 - 8.3.1 Accessing Cyber Talent into the Air Force.....65
 - 8.3.2 Education and Training within the Air Force66
 - 8.3.3 Education and Training Recommendations67
 - 8.4 Cyber Workforce Development.....68
 - 8.4.1 Cyber Warrior of the Future.....68
 - 8.4.2 Cyber Workforce Development.....69
 - 8.4.3 Cyber Workforce Recommendations.....70
 - 8.5 Conclusions.....70
- 9. Conclusion, Summary Findings and Recommendations71
- 10. References.....73

- Appendix A: Acronyms76
- Appendix B: Terms and Definitions79
- Appendix C: Cyber Vision 2025 Team and Senior Independent Expert Reviewer Group85
- Appendix D: Cyber Vision 2025 Working Meetings88
- Appendix E: Cyber Vision 2025 Terms of Reference89

Table of Figures

Figure 1.1: Strategic Alignment of *Cyber Vision 2025*2
 Figure 1.2: Cyberspace Vision Alignment.....3
 Figure 1.3: RFI Responses3
 Figure 1.4: Extensive Subject Matter Expert Engagement.....4
 Figure 1.5: Enduring Security Principles.....5
 Figure 1.6: Partnerships6
 Figure 2.1: Strategic Trends 1999-202512
 Figure 2.2: Attacks and Effects (Source: 2008 AF SAB Cyber Study).....17
 Figure 3.1: Air Force NIPRNet Email Storage Outpaced by Industry22
 Figure 5.1: Space Systems Software Growth (Source: SEI).....36
 Figure 5.2: Successful Space Cyber Intrusions.....39
 Figure 7.1: Agility and Resilience55
 Figure 7.2: Assess Risk and Assure Mission57

List of Tables

Table 1.1: Cyberspace S&T Desired Outcomes10
 Table 1.2: Cyberspace S&T Focus Areas11
 Table 2.1: Trends Threatening to the AF Mission.....20
 Table 3.1: S&T to Assure and Empower the Mission26
 Table 3.2: S&T to Enhance Agility and Resilience26
 Table 3.3: S&T to Optimize Human-Machine Systems27
 Table 3.4: S&T for Foundations of Trust.....28
 Table 4.1: Air Domain S&T Recommendations.....33
 Table 5.1: Space Domain S&T Recommendations40
 Table 6.1: Assuring and Empowering Cyber C2 and ISR.....47
 Table 6.2: Human-Machine Systems48
 Table 6.3: Resilience and Agility.....49
 Table 6.4: Foundations of Trust.....49
 Table 7.1: Enabling S&T for Cyberspace53

Cyber Vision 2025

1. Introduction

Cyber Vision 2025 is the Air Force vision for cyber Science and Technology (S&T) spanning the domains of air, space, cyber, Command and Control (C2), Intelligence, Surveillance and Reconnaissance (ISR), and mission support to address current and future threats. *Cyber Vision 2025* focuses on S&T in the near, mid and far term that will

advance the survivability, affordability, and effectiveness of AF operations. Building upon the July 2011 Department of Defense (DoD) *Strategy for Operating in Cyberspace*, the July 2010 Air Force Doctrine Document 3-12 on *Cyber Operations*, as well as *Technology Horizons* and Air Force Scientific Advisory Board cyberspace studies, *Cyber Vision 2025* articulates a way forward in cyberspace S&T and mission support. While not exhaustive, *Cyber Vision 2025* provides a critical starting vector and essential focus down a flight path to an assured cyber advantage.

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

Honorable Michael Donley
Secretary of the Air Force
23 March 2012



1.1 Motivation

Air Force systems are increasingly dependent upon cyberspace for both mission enablement and mission delivery. Simultaneously, cyberspace is an increasingly competitive and contested environment and may be characterized as denied in some parts of the world. In

addition, fiscal constraints are driving a need for efficiency. Unfavorably, we are human resource limited and will suffer from a limited future supply of domestic graduates in computer science. We are also resource limited in time given the speed of attacks and velocity of threat evolution. Finally, observing the appearance of worms such as Stuxnet, Duqu, and Flame or demonstrations of adversarial remote control of automobiles, cyber operations have moved beyond the virtual realm to touch the physical world. Notably, societies with cyber capabilities enjoy not only economic benefits but military power.

“Everything we do can be affected either by or through [cyberspace] in either a good or bad way.”

Gen Mark Welsh
Chief of Staff, U.S. Air Force
18 September 2012



1.2 Vision and Alignment

As illustrated in Figure 1.1, *Cyber Vision 2025* leverages and flows naturally from the Department of Defense *Cyber Strategy*, *AFDD 3-12 Cyber Operations*, the White House *Trustworthy Cyberspace* strategic plan, and strategic cyber studies

by the Air Force Scientific Advisory Board as well as the *Air Force Science and Technology Plan* and *Technology Horizons*. The formulation of *Cyber Vision 2025* carefully considered Air

Cyberspace Vision
Assured cyber advantage across air, space, cyberspace, C2, ISR, and mission support

Force focus on Global Vigilance, Global Reach, and Global Power, joint, interagency, combatant command (COCOM) and MAJCOM requirements, and Air Force Core Function Master Plans (CFMPs).



Figure 1.1: Strategic Alignment of Cyber Vision 2025

As illustrated in Figure 1.2, the Air Force cyber S&T vision aims to achieve the “Assured cyber advantage across air, space, cyberspace, C2, ISR, and mission support.” Each of these words bears important meaning. “Assured” means ensuring operations in spite of vulnerabilities in militarily, economically, and politically contested environments. The Air Force interest in “cyber” spans development, acquisition, and employment. The “advantage” the Air Force seeks is a readiness, robustness, and resilience edge over our adversaries to ensure operational supremacy. Finally, the Air Force requires cyber supremacy within and “across” the full spectrum of “air, space, cyberspace, C2, ISR, and mission support.” This vision is aligned with Air Force heritage focusing on strategic, global engagement. In cyberspace, this means a focus on Global Vigilance through global persistence and awareness, on Global Reach via global access, speed, and stealth, and on Global Power via integrated, cross domain effects. The later implies careful coordination of Air Force, joint and allied actions across air, space, land, sea, and cyberspace. An assured cyberspace advantage across air, space, and cyberspace is necessary across all lines of operation including exploitation, defense, and offense.

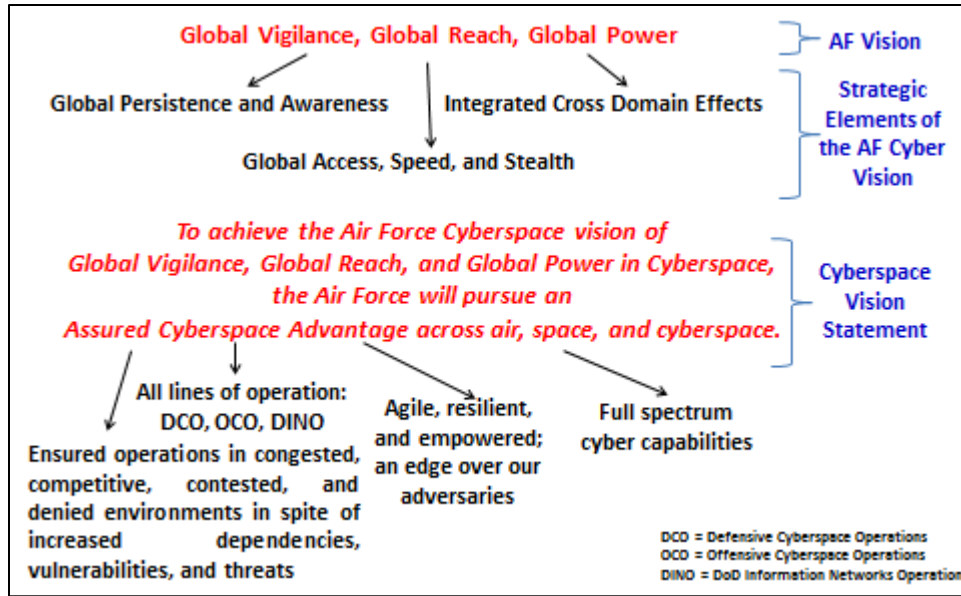


Figure 1.2: Cyberspace Vision Alignment

1.3 Methodology

The *Cyber Vision 2025* study was guided by a three star governance team and an enterprise wide set of key Air Force stakeholders (See Appendix C). It was organized into mission focused panels in each of the areas shown in Figure 1.1, collaboratively partnering senior experts and leaders from MAJCOMS, Air Force Research Laboratory (AFRL), product centers, operational units, and Headquarters Air Force. National, DoD, and Air Force strategy and policy provided guidance for areas of focus of attention. To engage external expertise, a public RFI resulted in over 100 detailed capabilities and technologies submissions (classified and unclassified) for consideration by the study. The mission area distribution of these is shown in Figure 1.3. The team made several focused site visits, including to Silicon Valley, as well as a classified cyber focused review with the National Laboratories. Multiple subject matter expert workshops/summits were held at major Air Force installations (See Appendix D), and included expert participants from industry, academia, government, National Laboratories, and Federally Funded Research and Development Centers (FFRDCs). We generalized a set of security principles based on practices from a broad range of institutions including but not limited to those shown in Figure 1.4. Expert teams (See Appendix C) incorporating operational and technical experts in air, space, cyber, C2, ISR and mission support assessed the very best of identified ideas and technologies, forecasted capabilities, and created an S&T focus in the near, mid and far term for each mission. A senior independent expert review group (Appendix C) peer reviewed the results in two major reviews at the Pentagon which were assessed by the senior governance council and approved by Air

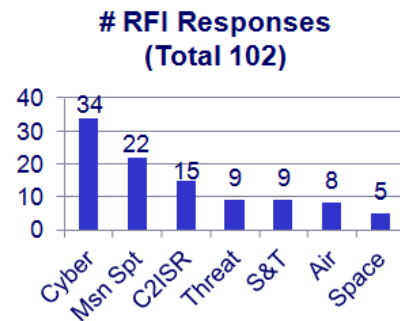


Figure 1.3: RFI Responses

Force leadership (See Appendix C), although given its dynamicity, complexity, and strategic role, cyberspace S&T will require continued planning and refinement.



Figure 1.4: Extensive Subject Matter Expert Engagement

1.4 Enduring Principles

As illustrated in Figure 1.5, our extensive outreach to experts provided a rich experience base from which to generalize several enduring concepts that have proven to mitigate risks across multiple organizations and promise to stand the test of time, particularly important in a rapidly evolving domain. These general security concepts can be tailored and employed in all missions by requirees, acquirers, developers, operators, and commanders. For example, by adhering to the principle of least privilege, users only receive permissions necessary to accomplish their mission (e.g., implementable by mechanisms such as discretionary access control, white listing, or using containers to limit functionality), reducing the opportunity for unintentional missteps or intentional mischief. And by distributing authority, employing peer review, or using two person rules, checks on power can be used to maintain balance of control. The principle of non-interference expresses the need for the assured separation of security levels as well as requiring that one operator not thwart the actions of another, achievable through careful coordination and synchronization of action. Minimization of attack surfaces by pursuing smaller solutions, limiting dependencies, or eliminating non-essential functionality can help reduce potential avenues of attack and/or vulnerabilities. Finally, simplifying systems (e.g., standard architectural interfaces, avoiding complexity) can reduce cost and risk. Systems can enhance their survivability by increased fitness/readiness/vigilance, improved intelligence and situational awareness, faster responsiveness, flexibility in reacting to a threat (cyberspace maneuver), and rapid evolution as threats and opportunities progress. If an attack cannot be avoided, resilience can be enhanced by a variety of ways including redundancy, alternate (e.g., wartime) modes, diversity of components, active defenses, and rapid reconstitution following a catastrophic attack. We found that some of the most successful organizations were able to integrate and

optimize defense with offense and tap into the appropriate mix of automation and human intelligence to allow them to achieve the proper balance between confidence in distributed operations and the need for detailed, centralized control. Finally, some of the best organizations leveraged limited talent, treasure, and time, by focusing on maximizing the benefits of their cyber posture (cost savings, efficiencies, and effectiveness) while maximizing the burden on the adversary (resources, risks, uncertainty) and/or denying them benefits, thus deterring attacks.

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 (coordination, synchronization)
Minimization	-limit attack surface, limit dependencies, eliminate non-essential functionality
Simplification	-allow only necessary complexity, employ standards (interfaces/controls)
Survivability	-fitness/readiness, awareness, speed (responsiveness), agility (e.g., flexibility/maneuver), and evolvability
Resilience	-robustness (e.g., redundancy), diversity, active defense, rapid reconstitution
Optimization	-offense/defense, human creativity and machine intelligence, cost/benefit
Leverage	-maximize adversary cost/risk/uncertainty and friendly benefit/assurance/efficiency

Figure 1.5: Enduring Security Principles

In addition to principles, a number of best practices were identified. For example, systems should design in redundancy, diversity, and roots of trust. Architectures should employ loose couplers between major elements (e.g., data exchange standards) to avoid the brittleness of customized and direct connections. Acquisition can be improved by demanding clear and focused requirements, early and continual user and test involvement, early prototyping and rapid cycles for evolution, modular/open standards, and model driven architectures. Similarly, incentivizing good cyber hygiene reduces a significant number of vulnerabilities. Encrypting data both at rest and in motion and ensuring chain of custody reduces the risk of information loss. Fractionating authorities can also reduce the likelihood of privilege escalation. Finally, focusing efforts on the acquisition, development and proper engagement of highly experienced cyberspace experts can significantly reduce risks.

1.5 S&T Partnerships

Given limited resources, the Air Force cyber S&T approach is to maximally leverage knowledge, capabilities, and investments in our sister services, departments, National Laboratories, industry and industrial consortia, utilities, Federally Funded Research and Development Centers, universities, and international partners as illustrated in Figure 1.6.



Figure 1.6: Partnerships

This approach allows the Air Force to preserve resources and focus investments on Air Force unique systems and missions. Examples where the Air Force will partner include but are not limited to the following organizations and investments:

- U.S. Cyber Command (USCYBERCOM) activities and investments in global cyber operations in support of joint and national missions
- U.S. Strategic Command (USSTRATCOM) expertise in cyber strategy and deterrence
- National Security Agency (NSA) leadership in cryptography and signals intelligence (SIGINT) and Central Intelligence Agency (CIA) **Information Operations Center expertise in foreign** state and non-state actors
- National intelligence community cyber intelligence tasking, collection, processing, analysis and dissemination capabilities
- Defense Advanced Research Projects Agency (DARPA), National Science Foundation (NSF), service laboratory and private sector investments in cyber research and human capital development
- National Aeronautics and Space Administration (NASA) and Federal Aviation Administration (FAA), and private sector investments in air and space vehicle autonomy as well as complex cyber systems command and control
- Department of Homeland Security (DHS) critical infrastructure protection expertise
- Department of Energy National Laboratories (e.g., Sandia, Los Alamos, Livermore)
- Public-private partnerships in cyber resilience, intelligence, and consequence management (e.g., Defense Industrial Base (DIB) Pilot)
- Public and private investments in information technology and critical infrastructure
- Joint DoD initiatives in resilient engineering and cyber research
- Academia pursuing innovations in cyberspace research and education

- Defense industrial base companies who focus Independent Research and Development (IR&D) dollars to joint Air Force / industry cyber initiatives
- Allies willing to engage in international partnerships (e.g., NATO, TTCP).

These partnerships and efforts are also facilitated through government coordination mechanisms such as the Assistant Secretary of Defense for Research and Engineering (ASD (R&E)) Cyberspace Priority Steering Council (PSC). Partnerships with these organizations will enable the Air Force to focus its efforts on unique air, space, cyber, C2 and ISR missions.

1.6 S&T Roles: Lead, Follow, Watch

To clarify partnerships, roles, and responsibilities, *Cyber Vision 2025* articulates priority technology investment areas by distinguishing among three key roles: technology leader (L), fast follower (F), and technology watcher (W). In a *technology leader* role (e.g., cyber embedded in air, space, missiles and munitions), the Air Force is a lead investor and creates or invents novel technologies through research, development and demonstration in areas that are critical enablers of Air Force core missions and associated platforms. In a *fast follower* role, the Air Force rapidly adopts, adapts, and/or accelerates technologies originating from external organizations who are leaders and primary investors in focused S&T areas as part of their core mission (e.g., national investments in cyber intelligence, commercial investments in high performance computing). In a *technology watcher* role, the Air Force uses and leverages others' S&T investments in areas that are not our primary or core missions (e.g., commercial commodity information technology, commercial communications, critical infrastructure such as power and water). Roles were assigned using the consensus of small groups of experts and stakeholders and could change depending upon resource, operational priority, or technology changes.

1.7 Strategic Focus

Consistent with Air Force heritage of Global Vigilance, Global Reach, and Global Power, the Air Force should emphasize strategic employment of cyber to achieve global effects, in concert with operations by sister services and coalition partners. Further mission focus is detailed in the classified version.

“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 and
Cyberspace Core Function Lead Integrator
AFCEA Cyber Symposium, 7 February 2012



1.8 Significant Past Progress

While Air Force cyberspace dependencies and threats are daunting, it is important to note that the service has made significant progress in policy, people, and processes in the last two years alone. In addition to standing up the 24th Air Force, the Air Force has published a Cyberspace Core Function Master Plan (CFMP), published AF Policy Directive (10-17) on Cyberspace Operations, established the AF-Cyber Integration Group (CIG) for coordination across the CFLI

and HAF, reported the Strategy for Cyberspace at CORONA TOP 2011, stood up the Cyberspace Operations and Support Community and drafted a Cyberspace Roadmap (A3/CIO A6 and AFSPC/CFLI). Moreover, in addition to establishing the 17D Cyberspace Operator career field, a 6 month long Undergraduate Cyber Training (UCT) was established and is in operation at Keesler AFB, Cyber 200 and 300 graduate courses have been stood up at AFIT, and a cyber Weapons Instructor Course (WIC) has been launched at Nellis AFB. In addition to the current AFIT Cyberspace Technical Center of Excellence (CyTCoE), USAFA, ROTC, and OTS programs that produce cyberspace officers, the Air Force participated in the first USCYBERCOM CyberFlag hosted at Nellis as well as a Red Flag live fire, incorporating for the first time air and space support of cyber, and force on force defense of the CAOC-N. AFRL has formulated a Cyberspace S&T Strategy that is aligned to the DoD Cyber Strategy and supportive of key elements of *Cyber Vision 2025*. Finally, AFCYBER warfighting forces have been employed in support of Air Force operations and USSTRATCOM/USCYBERCOM. While much has been accomplished, much remains to be done.

1.9 Cyber Vision 2025 Integrating Themes and Desired Outcomes

Four core, integrating themes are addressed throughout *Cyber Vision 2025*. These are mission assurance and empowerment, agility and resilience, optimized human-machine systems, and software and hardware foundations of trust. These directly leverage and extend the Office of Secretary of Defense Research and Engineering's Cyberspace Priority Steering Council strategy. Furthermore, they accelerate the DoD move toward a Joint Information Environment. We briefly describe each in turn and then summarize overall desired outcomes and focus areas.

1.9.1 Mission Assurance and Empowerment

Ensuring survivability and freedom of action in contested and denied environments requires enhanced cyber situational awareness for air, space, and cyber commanders. This can be enabled by automated network and mission mapping. Operators need to be able to detect and operate through cyber attacks supported by threat warning, integrated intelligence (e.g., SIGINT, HUMINT), and real-time forensics/attribution. Early vulnerability detection and enemy behavior forecasting can be enabled by high fidelity modeling and simulation, advanced cyber ranges, and cyber exercises. Operators also need support to achieve cross domain integrated effects as well as advances in cross domain measures of effectiveness (MOEs), including cyber battle damage assessment.

1.9.2 Agility and Resilience

Survivability in a contested cyberspace will demand an effective mix of redundancy, diversity, and fractionation (i.e., distributed functionality). System risk can be minimized by reduction of attack surfaces, segregation of critical mission systems, and attack containment. This can be enhanced by autonomous compromise detection and repair (self healing) and real-time response to threats. Advancing from signature based cyber sensors to behavior based detection will enhance attack detection. Active defense demands rapid cyber maneuver enabled by dynamic, randomizable, reconfigurable architectures (e.g., IP hopping, multilevel polymorphism).

1.9.3 Optimized Human-Machine Systems

Success in cyberspace demands the maximization of human and machine potential. This requires the 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 can enhance situational awareness, accelerate threat discovery, and empower task performance. Finally, autonomy must be appropriately distributed between operators and machines, enabled by increased transparency of autonomy and increased human “on the loop” or supervisory control.

1.9.4 Foundations of Trust

Operator trust in systems (e.g., sensors, communications, navigation, C2) can be enabled by secure foundations of computing including trusted foundries, anti-tamper technologies, and supply chain assurance, as well as effective mixes of government, commercial off the shelf, and open source software. Security can be improved by advancing formal verification and validation of complex, large scale, interdependent systems as well as advancing vulnerability analysis, automated reverse engineering, and real-time forensics tools. High speed encryption, quantum communication and, eventually, quantum encryption will further increase the confidentiality and integrity of supporting infrastructure.

1.9.5 Overarching Cyberspace S&T Desired Outcomes and Recommendations

Table 1.1 summarizes the near-, mid-, and far-term S&T desired outcomes where the Air Force should lead (L), follow (F), or watch (W) in cyberspace across the domains and mission areas of air, space, cyberspace, command and control, and ISR. For example, to assure and empower the mission requires an ability to provide, in the near term, semi-automated network and mission mapping and automated anomaly resolution, in the mid term, real-time situational awareness and command and control of our networks, and in the far term, autonomous mission assurance and management. Similarly, to ensure agility and resilience in cyberspace will require, in the near term, fractionated, morphable, reconstituting architectures and active cyber maneuver, in the mid term, automated vulnerability detection and mitigation, and in the far term, secure, autonomous communications and networks. To optimize human-machine systems, in the near term we will need to advance operator selection and measurement and adversarial modeling, in mid term we will need to assess and augment human performance, and in the far term we must optimize operator performance. Finally, hardware and software foundations of trust will demand advances in reverse engineering and anti-tamper, verification and validation to ensure integrity, and quantum methods and provable assurance to provide trust and mitigate contested environments. In subsequent sections of this document, detailed cyberspace S&T vectors for air, space, cyberspace, command and control, and ISR missions are motivated and articulated.

Table 1.1: Cyberspace S&T Desired Outcomes
Technology Leader (L), Follower (F), Watcher (W)

Area	Near (FY12-FY15)	Mid (FY16-20)	Far (FY21-25)
Assure and Empower the Mission	<ul style="list-style-type: none"> • Semi-Automated Mission Mapping and Anomaly Resolution for Cyber SA (L) • Secure Communication (L) • Access and D5¹ Cyber Effects (L/F) 	<ul style="list-style-type: none"> • Real-time AFNET SA & C2 (L) • Cyber Mission Verification and Assurance Across Sensors/Platforms • Survivable C3 (L) • Advanced Access, D5 Effects (L/F) 	<ul style="list-style-type: none"> • Autonomous Cyber Mission Assurance/ Management (L) • Predictable Cyber Effects on Mission Systems (L)
Enhance Agility and Resilience	<ul style="list-style-type: none"> • Fractionated², Morphable, Reconstituting Architectures (L) • Cyber Maneuver (L) • Intelligent Mix of GOTS/COTS (F) 	<ul style="list-style-type: none"> • Online Vulnerability Identification and Adaptation (F) • Resilient Virtualization (F) 	<ul style="list-style-type: none"> • Autonomous, Secure, Agile Composable CyberPhys Sys (L) • Cognitive Comm/Networks (agile, reconfigure, self heal) (L)
Optimize Human-Machine Systems	<ul style="list-style-type: none"> • Operator Selection (e.g., traits, methods) (L/F) • Operator Measurement (e.g., stress, cognition, perf., trust) (L) • Adversarial/Social Modeling (L) 	<ul style="list-style-type: none"> • Automated Individual Performance Assessment and Training (L) • Initial Augmented Cognition (L) • Auto Cyber Battle Damage Assess (L) 	<ul style="list-style-type: none"> • Intent/Behavior Detection and Forecasting (L) • Human-Machine Perf Optimize (L) • Neuroscience based brain computer interfaces (L/F)
Foundations of Trust	<ul style="list-style-type: none"> • Measurement, Vulnerability Model/Analysis, & Verification (L) • Real-Time Cyber Reverse Engineering (L/F) • Software Anti-Tamper (L) • Secure Virtualization (F) 	<ul style="list-style-type: none"> • Information Integrity V&V • Quantum Communication (L) • Root of Trust for Cyber C2 (L) • Embedded Anti-Tamper (F) • Semi Autonomous Supply Chain Assurance (F) 	<ul style="list-style-type: none"> • Quantum Methods for V&V, Trust, and Vulnerability Assessment (F) • Provable Mission Assurance in Contested Domains (L)

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

²Fractionated = physically and functionally distributed

Using the outcomes identified in Table 1.1, Table 1.2 summarizes focus areas using color coding to indicate a primary (red), secondary (yellow) or tertiary (green) focus. In both instances of green in Table 1.2, the Air Force is primarily a follower of industry leadership. Yellow areas enjoy some current investment but require additional effort. For example, cyber access and affects are enabled by the SCOTI (Selective Cyber Operations Technology Integration) AFRL flagship capability, however, this is currently only in a pilot phase. Finally, areas of primary emphasis are indicted in red. For example, while the Air Force currently has some operational capabilities such as IP hopping to provide a degree of network agility, increasing the fractionation and morphability of Air Force computing architectures will increase resiliency. Near, mid, and far-term S&T recommendations are further addressed in subsequent sections.

1.10 Structure of Cyber Vision 2025 Document

In the remainder of this document, after articulating the future environment and forecasted threat space, *Cyber Vision 2025* addresses each key Air Force area in turn: cyberspace, air, space, C2, ISR, and mission support. Each domain section details that mission environment, outlines core cyber needs of that mission, makes key mission-specific observations, recommends actions to ensure the cyber advantage in that mission area, and provides a technology focus in the near (1-5 years), mid (6-10 years), and far term (10-15 years). Finally, enabling technologies that promise advances across two or more Air Force mission areas are detailed. The document concludes by recommending a way forward.

Table 1.2: Cyberspace S&T Focus Areas

■ Primary
■ Secondary
■ Tertiary

Area	Near (FY12-FY15)	Mid (FY16-20)	Far (FY21-25)
Assure and Empower the Mission	<ul style="list-style-type: none"> • Semi-Automated Mission Mapping and Anomaly Resolution for Cyber SA (L) • Secure Communication (L) • Access and D5 Cyber Effects (L/F) 	<ul style="list-style-type: none"> • Real-time AFNET SA & C2 (L) • Cyber Mission Verification and Assurance Across Sensors/ Platforms • Survivable C3 (L) • Advanced Access, D5 Effects (L/F) 	<ul style="list-style-type: none"> • Autonomous Cyber Mission Assurance/ Management (L) • Predictable Cyber Effects on Mission Systems (L)
Enhance Agility and Resilience	<ul style="list-style-type: none"> • Fractionated, Morphable, Reconstituting Architectures (L) • Cyber Maneuver (L) • Intelligent Mix of GOTS/COTS (F) 	<ul style="list-style-type: none"> • Online Vulnerability Identification and Adaptation (F) • Resilient Virtualization (F) 	<ul style="list-style-type: none"> • Autonomous, Secure, Agile Composable CyberPhysical Sys (L) • Cognitive Comm/Networks (agile, reconfigure, self heal) (L)
Optimize Human-Machine Systems	<ul style="list-style-type: none"> • Operator Selection (e.g., traits, methods) (L/F) • Operator Measurement (e.g., stress, cognition, perf., trust) (L) • Adversarial/Social Modeling (L) 	<ul style="list-style-type: none"> • Automated Individual Performance Assessment and Training (L) • Initial Augmented Cognition (L) • Auto Cyber Battle Damage Assess (L) 	<ul style="list-style-type: none"> • Intent/Behavior Detection and Forecasting (L) • Human-Machine Perf Optimize (L) • Neuroscience based brain computer interfaces (L/F)
Foundations of Trust	<ul style="list-style-type: none"> • Measurement, Vulnerability Model/Analysis, & Verification (L) • Real-Time Cyber Reverse Engineering (L/F) • Software Anti-Tamper (L) • Secure Virtualization (F) 	<ul style="list-style-type: none"> • Information Integrity V&V • Quantum Communication (L) • Root of Trust for Cyber C2 (L) • Embedded Anti-Tamper (F) • Semi Autonomous Supply Chain Assurance (F) 	<ul style="list-style-type: none"> • Quantum Methods for V&V, Trust, and Vulnerability Assessment (F) • Provable Mission Assurance in Contested Domains (L)

2. Future Environment and Cyberspace Threat

We forecast the world in 2025 along multiple interacting dimensions. We looked at changes in demographics, the economy, generalized technology topics, and threats because these themes will significantly impact the resources, energy, and requirements for not only the technological developments of the future but also the role cyberspace will play in this new world. Having envisioned this world, we then examined technology specific trends that we see serving this vision (see Figure 2.1) and overlaid cyberspace from an adversarial side to its impact on society as a whole.

2.1 Demographics, Economy, and Adversaries - 2025

Demographic trends will likely influence how cyberspace capabilities evolve around the globe with respect to both R&D investment and the application of capabilities. In 2025, it is expected that 56% of the world’s 8 billion people will reside in Asia—making it an attractive commercial market for advanced information technologies. Additionally, the world's population is also an aging population; in 2000, approximately 10% were over 60 years of age. By 2025, that figure will likely increase to 12.5% and, by 2050, it will be close to 21.5%. In some parts of the world (e.g., Japan), this aging population trend is already pushing the development of robotic systems to help meet their growing health care demands.

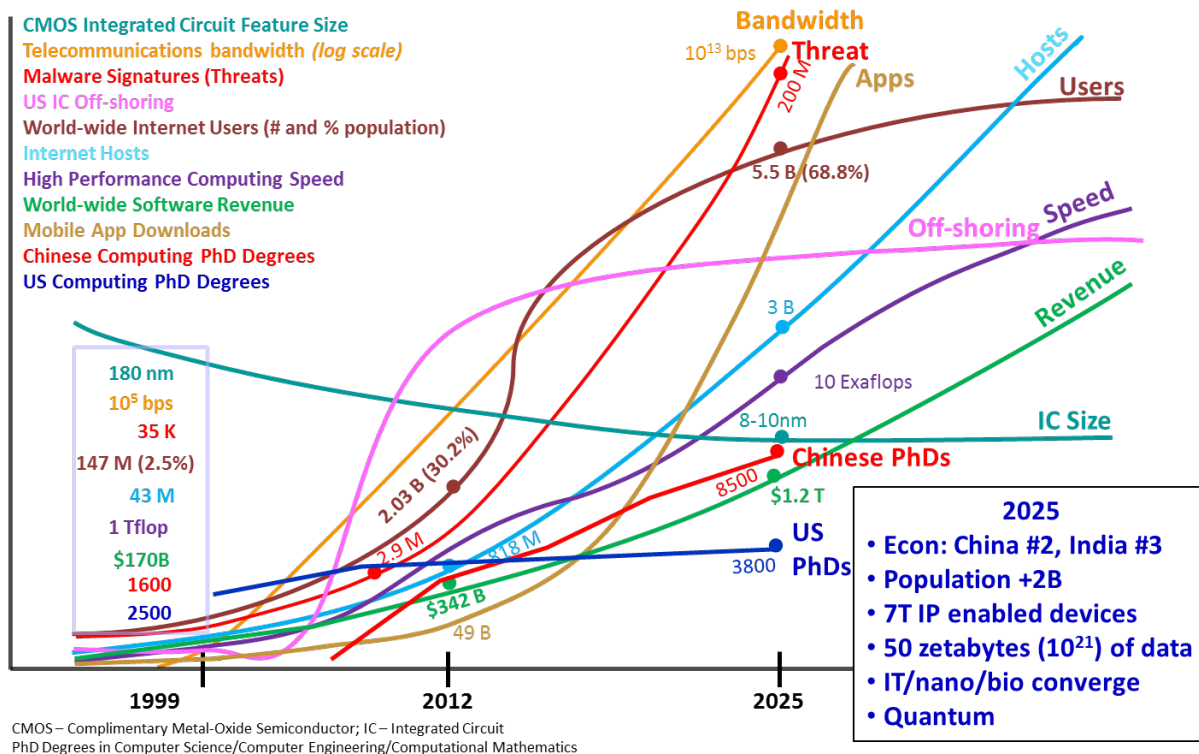


Figure 2.1: Strategic Trends 1999-2025

Although it is difficult to comprehend the amount of change exhibited in the cyber domain in just the past 10 years, the technology trends highlighted in Figure 2.1 suggest that we have just

begun to scratch the surface. For example, by 2025 there will be an estimated 5.5 billion people online using 25 million applications, engaging in billions of interactions per day, and creating 50 zetabytes (trillion gigabytes) of data. Supercomputers will be able to sustain operations at the 10 ExaFLOPS (10^{18} floating point operations per second) level and new devices will have replaced today's traditional Complimentary Metal-Oxide Semiconductor (CMOS) devices.

The nature of the threat will also change as globalized economic forces and competition play out, likely increasing multi-polarity in the geopolitical landscape, shifting country alliances (most likely a consequence of limited resources, e.g., water, energy, etc.) as well as creating many additional anonymous actors who are difficult to retaliate against. Although the International Monetary Fund (2011) reports that China will have the #1 economy as early as 2016, the National Intelligence Council (2008) forecasts that China will still be #2 in 2025, followed by India. As China and India's economies grow, the United States will have significantly reduced political influence, particularly in Asia.

Additionally, "hybrid adversaries" that combine irregular tactics with advanced stand-off weaponry will be present that drive the United States and its allies to adapt their military forces to accommodate a wide-range of military contingencies from irregular forms of conflict against non-state actors, to state-sponsored hybrid combatants, to traditional forms of interstate conflict.

2.2 Technological Change - 2025

Technology development and deployment will accelerate through 2025 and the nature of the threat will be continually evolving. To highlight just a few relevant technologies, there may be bots that can reason on their own and evolve to evade updated security software. Social computing will be advanced and applied extensively to predict (and likely interdict or influence) social behaviors and emerging social patterns. Ubiquitous sensing will be wide spread with the continued miniaturization and proliferation of sensor technology.

Specific to cyberspace, in 2025, there will be a convergence of info-, nano-, and bio-technologies. The nature of devices will dramatically change, having moved from small mobile devices and augmented reality towards physical human-machine integration. The nature of secure communications and computing will have also changed with the fielding of secure quantum communication networks and small-scale quantum computers (i.e., some minimal number of qubits will be in use). Additional information is available in the classified Annex.

Figure 2.1 captures general lines of acceleration for various technologies. All but one line has an increasing slope meaning, in general, that by 2025 there will be:

- An alarming growth in malware threats
- A likely shift in United States integrated circuit (IC) off-shoring
- Vastly expanded number of Internet users and hosts
- Faster computers and data transfer rates
- Steadily growing software revenues

- Exponential growth in mobile application downloads.

Each technology trend will have an impact on the cyberspace environment of 2025, primarily in terms of the quantity of people, activities, and data operating in and around cyberspace, and are discussed below.

CMOS Integrated Circuit Feature Size - If the current trend continues, CMOS Integrated Circuit feature size will reach 8-10 nm by 2025. Semiconductor manufacturing processes have continued to steadily improve in the miniaturization of integrated circuits from a feature size of approximately 180 nm in 1999 to ~22 nm in 2011. According to the Air Force *Energy Horizons* study, recent progress in chip fabrication presents tremendous opportunity to continue improving density and power efficiency. These improvements will result in a significant reduction in the size and an increase in the capability of future commercial and military devices which promote increased energy savings.

Telecommunications Bandwidth - The rate at which users can move data will reach 10^{13} bps. This is extrapolated from known data for 1980 through 2010. This is a large amount of data and can be illustrated by a simple example: in 2012, a consumer can purchase a 1 Terabyte drive; by 2025, network configurations will provide the consumer the ability to transmit ten of those external hard drives every second.

Malware Signatures - Estimates indicate that by 2025 there will be roughly 200 million new malware signatures per year. This estimate is based on historic data reported from 1999 through 2010, which indicates a general exponential growth rate. The estimate is highly vulnerable to a large number of variables that could drastically effect estimates as far out as 2025. These variables include:

- New technology that makes malware less effective and thus less desirable to produce
- New wide-spread technology that is vulnerable to malware (e.g., smart phones)
- Explosive growth of Internet-enabled devices (e.g., handheld, medical equipment, etc.)
- Changes in software development practices that increase or decrease vulnerabilities
- The number of new Internet users lacking disciplined computer security practices

U.S. Integrated Circuit Off-shoring – In 2005, the Defense Science Board Task Force on High Performance Microchip Supply called for initiatives to ensure affordable and assured supply of trusted microelectronics produced domestically. It is difficult to predict whether the current United States trend of the off-shoring of the design and fabrication of integrated circuits will continue. However, there are four primary reasons companies locate value-chain activities offshore: access to location, specific resources (especially engineering talent), cost reduction, and access and development of local market share. The impact of continued off-shore production of any technology is the lack of control over quality, quantity, and authenticity (See GAO 12-375). This lack of control can have serious effects for our national security by calling

into question the confidentiality, integrity, and availability of all of our information technology based infrastructure.

World-wide Internet Users - Estimates indicate that the maximum possible Internet penetration rate is 80% of the world's population; the United States reached this penetration rate with respect to its population in 2010. It is unknown if Internet use will reach the 80% mark in 2025; it has been estimated that there will be 5.5 billion Internet users in 2025, which is 68.8 % of the world's estimated 8 billion people. The combination of home, industrial and medical devices requiring network connectivity is expected to result in approximately 7 trillion IP-enabled devices by 2025.

Internet Hosts - Internet hosts are expected to number roughly 3 billion in 2025. Internet hosts are roughly equivalent to Internet domains (e.g., google.com, af.mil, etc.) but do not include individual websites within each domain. Each domain will have the ability to host thousands of unique websites.

High Performance Computing Speeds - By 2025, processing speeds of high performance computers are expected to reach 10 ExaFLOPS. Currently the world's fastest supercomputers operate at speeds above a thousand trillion floating point operations per second (PetaFLOPS). Realization of computing speeds surpassing one quintillion floating point operations per second (ExaFLOPS) may be reached by 2018, and 4 ExaFLOPS is expected before the end of the decade. The next step will be to reach ZettaFLOP (one sextillion FLOPS) speeds, which most estimates indicate will occur around 2030.

Worldwide Software Revenues - Revenues from worldwide software sales are expected to increase to \$1.2T in 2025. This estimate is based upon current trends in commercial software revenue, and includes both Software-as-a-Service and packaged software sources of revenue. This does not include Free and Open Source Software (FOSS) growth.

Global Mobile Application Downloads - The current exponential growth in global mobile application downloads and associated potential for criminal data theft is expected to continue. The number of mobile application downloads was estimated to increase from 8 billion in 2009 to just less than 50 billion in 2012.

Advanced Academic Degrees - The number of PhD degrees awarded annually in computer science, computer engineering, and computational mathematics to United States students is expected to roughly flat line in 2025 at 3,800 whereas in China, the number is expected to grow to 8,500. Additionally, of students receiving advanced degrees in the United States, less than half are expected to be United States citizens. Without a well educated workforce, the United States will fall behind in technology advances that contribute to offensive and defensive capabilities in the cyber domain. Those same technology advances provide intellectual property rights to the originator; if the United States is not making those technological advances, another

country will be setting and controlling standards and advancements in an area that may be critical to our national security.

2.3 Impacts

The malware signature and mobile application download trends could have adverse effects on the global economy. New malware will have a potential economic impact if the population's source of income is affected by a disruption of the banking, transportation, or infrastructure systems. Likewise, the criminal data theft from downloading of mobile applications will potentially affect the economic well being of individuals, and countries will have to deal with the ramifications. Rapid growth in telecommunication bandwidth, number of worldwide Internet users, the number of Internet hosts, and high performance computing could have political and economic effects. All contribute to the free and rapid dissemination of information, thereby making it more difficult for repressive regimes to control what is released to the media and to the public. The overall impact of the environment in 2025 is that cyberspace will be increasingly integrated into the United States Air Force (USAF), our adversaries' capabilities, and society in general. Dependency on information technology (IT) systems coupled with evolving cyber threats will force the USAF to adapt to successfully operate in an increasingly congested, contested, and competitive cyberspace environment.

2.4 Cyber Threats to Air Force Missions

The USAF faces rapidly evolving and increasingly advanced cyber threats as nearly all mission logistics, planning, and execution depend on a domain which forces the USAF to operate in a congested, contested, and competitive cyberspace environment. The capability of foreign cyber actors ranges from those with minimal access and expertise to full-scope actors. Offensive Cyberspace Operations (OCO) actors can threaten USAF missions employing a range of methods of attack (e.g., social engineering, malicious insider, supply chain) by attacking a range of interdependent layers with a range of effects on availability, integrity, and confidentiality, as illustrated in Figure 2.2.

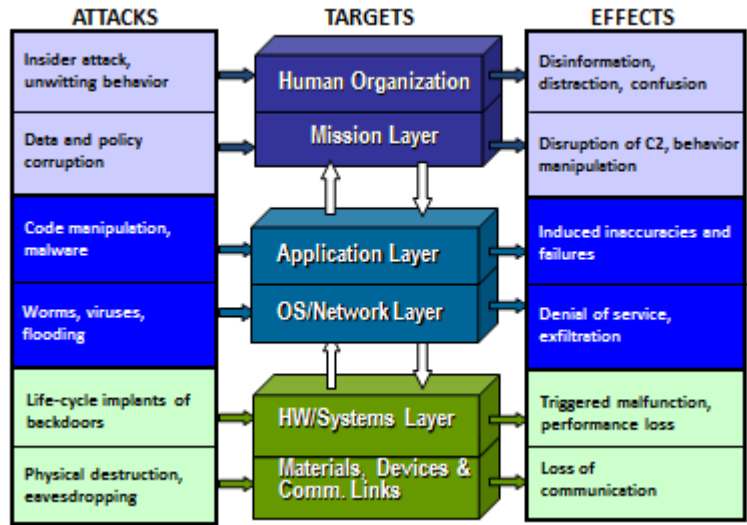


Figure 2.2: Attacks and Effects
 (Source: 2008 AF SAB Cyber Study)

Attackers can undermine supporting critical infrastructure (e.g., power, water, and fuel), hardware, software, firmware, Command and Control (C2), Intelligence, Surveillance and Reconnaissance (ISR) systems, or directly attack mission systems via the computing capabilities embedded in air and space platforms. Moreover, our missions systems are increasing interconnected, with all vulnerable to the weakest link. Notably, the FBI has reported that 90% of current cyber attacks start with spear phishing, making the operator a prime direct target. The threat from both state and non-state cyber actors will continue to increase as advances in – and the growing dependency on – IT and embedded software underpin the mission.

2.4.1 Threat Vectors

The cyber attack surface of the USAF mission is susceptible to a wide variety of attacks categorized by three specific and unique vectors: supply chain, malicious insiders, and foreign actors.


2.4.1.1 Supply Chain Vector

The supply chain threat vector focuses on opportunities for attack during the manufacturing and movement of materials as they flow from their source to the end customer. Supply chain includes purchasing, manufacturing, warehousing, transportation, customer service, end of life, demand and supply planning, and supply chain management.

It consists of the people, activities, information, and resources involved in moving a product from its supplier to customer. Because of its complexity, the supply chain provides multiple

“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),
 Director of National Intelligence, 31 Jan 2012.



opportunities for those with malicious intent to contaminate the building blocks of integrated circuit devices necessary for the production of cyber related components. The manufacturing phase is a particularly attractive and vulnerable target for actors intent on disrupting computer operation, gathering sensitive information, or gaining unauthorized access to computer systems. Specifically, off shore production of integrated circuit components and software at facilities not approved as trusted foundries increases the likelihood that malicious, sub-standard, or counterfeit IT components and software will penetrate systems, networks and platforms vital to the USAF mission. Supply chain attacks are often used as a means to decrease mean time between failures, resulting in diminished availability and trust in USAF platforms and systems, or through infiltration of malicious instruction and/or additional features built into the architecture, which can be activated through simple environmental and/or circumstantial triggers. Finally, risk can also come simply from poor cyber hygiene, lax manufacturing processes, or criminal efforts to profit from counterfeit components.

2.4.1.2 Malicious Insider Vector

Malicious insiders include both willing and unknowing participants, who have legitimate access to an organization's information systems, and deliver malicious software or corrupt data to critical mission systems. Willing participants, exhibiting a range of motivations (greed, revenge, ideology), adversely impact an organization's mission by taking actions that compromise information confidentiality, integrity, and/or availability. Equally damaging, unwitting participants may unintentionally create or enable cyber vulnerabilities through poor cyber hygiene (e.g., poor information assurance practices or lack of operational security measures).

2.4.1.3 Foreign Actor Vector

The foreign actor is defined as a cyber actor with the capability and intent to conduct OCO, comprised of Cyber Enabling (CE) and/or Cyber Attack (CA) against the United States and its allies. We characterize CE as Advanced Persistent Threat (APT) and associate CA to state-sponsored or state-sanctioned Foreign Offensive Cyber Forces. The foreign actor vector leverages CE to exfiltrate strategically, operationally, and/or tactically relevant data and to prepare the battlespace for CA, then employs CE again to assess the effectiveness of CA.

Table 2.1: Trends Threatening to the AF Mission

Threat Area	Susceptibility Concerns – Cyber Attack Surface
Platform IT	Increasing embedded data processing systems throughout AF mission platforms does not constitute a secure closed network isolated from pervasive cyber threats.
Bring Your Own Device (BYOD)	AF personnel demanding to stay current and more effective while circumventing slow acquisition process and reducing acquisition costs by bringing in their own devices increases AF cyber attack surface as <i>unaccredited</i> devices are brought into <i>accredited</i> AF environments.
Embedded Processors	Replacing mechanical functions with software-driven operations increases the attack surface for malicious code/exploits and undesirable functionality injection into physical devices.
Software-driven Failure Modes	Performing critical operations via millions of lines of code increases the attack surface as the ability to validate software functionality exceeds capability.
Reliance on Industrial Control Systems (ICS)	Replacing physical controls and access with remote IT control systems that rely on network connectivity and software/hardware functionality, which were not designed for the current cyberspace environment, drastically increases the AF cyber attack surface.
Cloud Computing	Secure cloud computing environment for securing the AF mission is untried and complex, resulting in potentially large attack surfaces in which subscribing organizations typically share components, resources and security with other ‘trusted’ subscribers.
Android’s Law (Shrinking Android manufacturing cycles; 9.7 to 6.7 months)	The desire to incorporate the latest IT hardware and software advancements in support of network centric mission operations is resulting in new operating systems and hardware being introduced faster than their vulnerabilities can be identified and mitigated.
Moore’s Law (transistors on a chip doubles every 18 months)	The dependence on increasing processing power in support of mission logistics, planning and execution provides cyber actors with greater capability and an expanding suite of tools compounded with an increasing ease of mobility.
Quantum Communication and Encryption	The employment of quantum technologies will provide enhanced capabilities to AF computing and communications while simultaneously posing significant challenges to AF cyber security.

2.4.2 Areas of Concern: Threat Increase and Attack Surface Expansion

Cyber operations against USAF systems, networks and platforms are deliberate and unrelenting. The global ability to rapidly and accurately attribute detected OCO remains immature. Industry and academia have acknowledged that cyber threat capabilities often far outperform established defenses. According to the Director of National Intelligence document, “Unclassified Statement for the Record on the Worldwide Threat Assessment of the United States Intelligence Community for the House Permanent Select Committee on Intelligence,” dated 2 February 2012, “innovation in functionality is outpacing innovation in security and neither the public nor private sector has been successful at fully implementing existing best practices.” Thus, an area of great concern is the USAF’s ability to maintain rapid and accurate detection of foreign OCO in a contested and congested cyberspace domain. Trend analysis through 2025 reveals exponential growth in worldwide Internet users and threatening malware. Table 2.1 identifies

specific areas where the USAF should focus on global S&T trends, changes to the cyber attack surface, and potential threats to USAF mission.

2.4.3 Cyber Operations (CO) Actors in 2025 - Refer to classified Annex.

2.4.4 Threat Recommendations

To best posture the USAF's threat awareness and increase the cost of adversary OCO for the projected cyber environment of 2025, we recommend:

- More effective use of Title 10/50/32 in support of the USAF's strategic cyberspace mission
- Allocate USAF and Intelligence Community (IC) resources based on national and defense priorities with an emphasis on USCYBERCOM's Operational Directive 12-001
- Grow investment in cyberspace Scientific and Technical Intelligence (S&TI) and Foreign Material Exploitation (FME) capabilities.

2.4.4.1 More effective use of Title 10/50/32

While the USAF has established some integration of Title 50 and Title 32 functions and resources with Title 10 activities, these tend to be tactical in nature and limited to DCO of USAF networks. Improved integration is needed to adequately assure national-security missions and fully support non-kinetic target planning at the strategic level. Stronger integration of Title 10, 50, and 32 roles and responsibilities is recommended to produce and utilize *strategic intelligence* for the USAF's missions that depend upon air and space platforms and the supporting C2 and ISR systems. The IC needs the ability to create intelligence to enable mission planning for USCYBERCOM and the Service Components. Additionally, the IC needs to work closer with the acquisition community, including cleared defense contractors, to identify threats, risks and consequences of illicit intrusions. The current process of supplying the acquisition community with static cyber threats via System Threat Assessment Reports (STARs) is inadequate. System and platform developers need early and relevant integration of threat intelligence to mitigate risks associated with system vulnerabilities arising from adversary access, intent, capability and system susceptibility. This includes support of the cyber acquisition community, including consideration of embedded cyber components in air and space systems. Furthermore, the unique authorities and additional Air National Guard manpower provided by Title 32 could add cyber capabilities beyond what Title 10 and Title 50 resources could accomplish alone. The enhanced Title 10/50/32 integration must also work to determine if "anomalies" experienced by systems during operations (e.g., loss of a command link) are in fact foreign OCO. (OPR: AF/A2, OCR: AFSPC, SAF/AQ, AFMC)

2.4.4.2 Align USAF resources to USCYBERCOM Directives

In a purposeful measure to align cyberspace efforts and capabilities across the Service Components, USCYBERCOM issued Operational Directive 12-001 (APR 05 2012) which assigns roles and responsibilities to AFCYBER to identify requirements for, and advocate for the development of, cyber capabilities and TTPs for specific target sets. Alignment of USAF

efforts along functional lines is recommended to produce required S&T intelligence to achieve timely, efficient, and effective support to combatant command specific cyberspace operations. Title 10, 50, and 32 resources are essential to generation of cyberspace preparation of the battlespace efforts, both within the USAF and at the national IC level. OPR: AFSPC (24 AF), OCR: AF/A2 (AFISRA)

2.4.4.3 Invest in Cyberspace S&TI and FME

Currently, foreign materiel exploitation (FME) is assigned and performed by each service's intelligence production center based on the type of equipment - air and space systems are exploited by USAF, ground systems by the Army, and maritime systems by the Navy. Foreign cyber systems are not assigned to any particular Service Component, which leads to the potential for multiple services and IC organizations to conduct FME on the same components and devices. For example, FPGAs are used within foreign military systems of all service components and are key to determining capabilities, performance and cyber vulnerabilities. Reverse engineering such complex data devices is difficult and resource intensive. The assignment of unique responsibilities is paramount to efficient and timely exploitation in support of U.S. OCO. USAF is currently ahead of the other Service Components in the area of cyber FME. USAF should study the resource requirements and policy implications of the Air Force becoming the lead service for cyber FME. (OPR: AF/TE, OCR: AF/A2)

3. Cyberspace

3.1 Cyber Domain Strategic Context

The United States Air Force's capacity for Global Vigilance, Reach, and Power is enabled by a global networked information infrastructure known as cyberspace, much of which is connected to, and a part of, the Internet that links billions of users worldwide. The Department of Defense and especially the U.S. Air Force, given its global reach, have embraced net centric warfare in their missions to protect our country. The global cyberspace, a man-made domain, is growing at an exponential rate (doubling in size every two years) as a result of the confluence of technological breakthroughs and mass markets. By 2015, there will be 15 billion devices operated by 3 billion individuals (40% of the global population) passing 1 Zettabyte (10^{21}) of traffic a year¹. Such growth rates rapidly outpace DoD procurements and policies which move at a relatively glacial pace of 7-10 years. The email example of Figure 3.1 is but one instance of the problem.

U.S. Air Force missions in air, space, and cyberspace (and supporting command and control (C2), intelligence, surveillance, and reconnaissance (ISR) missions) are inextricably integrated with, and enabled by an intricate communications network infrastructure that is a part of the global cyberspace. While cyberspace affords and enables many useful capabilities and opportunities, connecting our national and military infrastructures, it also provides access

¹ Cisco Visual Networking Index: Forecast and Methodology, 2010-2015, June 2011

opportunities to our defense systems by practically anyone from any point on the globe. Interconnectivity through cyberspace has exposed previously isolated critical infrastructures vital to national security, public health, economic well-being, and AF missions. Cyberspace provides unique global reach and access unconstrained by distance, time, terrain, and borders connecting our national and military infrastructures. Cyberspace has the potential to deliver a full range of effects from the tactical to the strategic, and has become an integral part of the AF missions across the air, space and cyber domains. Conversely, cyberspace provides asymmetric avenues of attack for both nation states and non-state actors.

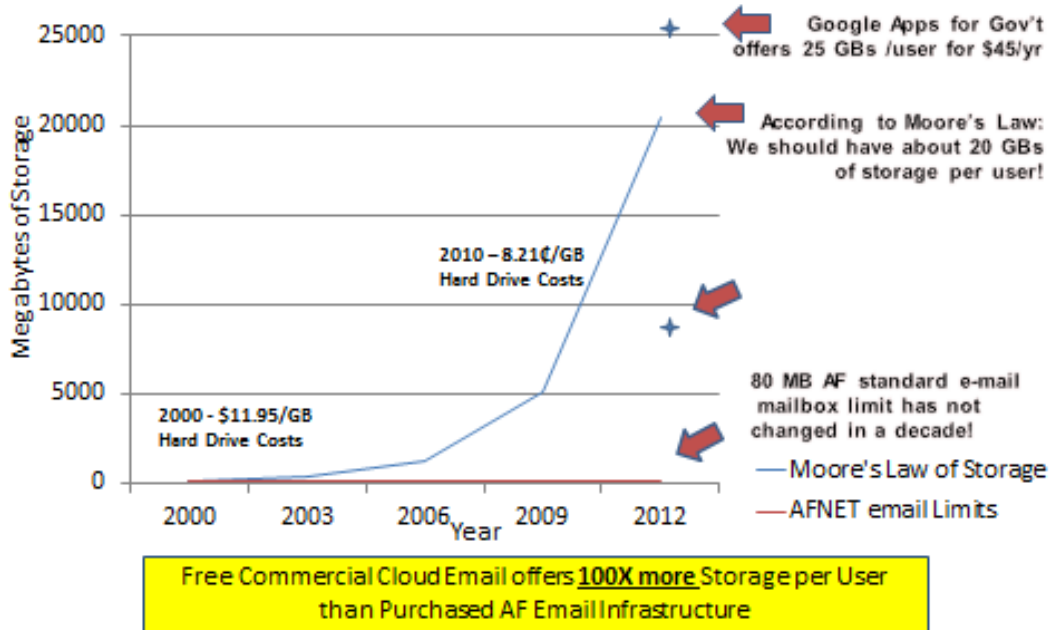


Figure 3.1: Air Force NIPRNet Email Storage Outpaced by Industry

More than any other technology, cyber technology and our adversaries' nefarious use of it evolves rapidly and often in unpredictable and complex ways. Adversaries may attempt to deny, degrade, deceive, disrupt, or destroy critical infrastructures and AF missions through cyberspace attack, thus affecting our warfighting systems and the nation as a whole. Conducting cyber-attacks is a relatively inexpensive endeavor with potential for high yield effects and no attribution. Commercial security firms report that the application, sophistication and frequency of cyber-attacks continue to grow at an alarming rate. Game changing technologies like the Stuxnet, Duqu, and Flame malware now exist. The malware's evolution suggests development is ongoing and may have affected its targets in ways not yet known. We have witnessed these technologies breaching what were once considered impenetrable networks. To counter rapidly evolving cyber threats, Air Force S&T must work directly with the AF cyber operational and acquisition communities to understand rapidly emerging requirements, address urgent needs, and streamline the development, test, and transition of cyber capabilities.

Most commercial sector research and development of cyber protection technologies is driven by private sector needs and not Air Force mission requirements. Commercial industry is primarily driven by profit and this drives the trade-off they will make to ensure the hardware and software in their manufacturing supply chains are free from viruses, back doors, and covert communications channels. The business case for commercial industry does not support the level of security required in AF weapon systems. The Air Force must work with industry to make Air Force priorities and security requirements known. In cases where industry developments fall short, the AF needs to identify the gaps and invest in the science and technology to develop capabilities to protect the information infrastructure critical to AF missions.

The Air Force S&T Strategy 2010 and the Air Force Chief Scientist's report on *Technology Horizons* stress the critical importance of cyber capabilities to the Air Force. Current AF S&T cyber capability requirements and priorities are based on the Air Force Space Command's 2011 Operational Need Statement. Key cyber capability areas for the Air Force are (1) passive defense, (2) defensive counter cyberspace, (3) cyberspace intelligence, surveillance and reconnaissance (ISR) & situational awareness (SA), (4) persistent network operations, (5) data confidentiality & integrity systems (DCIS), (6) cyberspace operations center, (7) offensive counter cyberspace, (8) contingency extension, and (9) influence operations.

The Air Force is challenged to assure and empower full spectrum cyberspace missions built upon trusted, resilient, and affordable cyberspace foundations. A prudent strategy would be to first establish trusted foundations within cyberspace and then build mission capability on top of those enhanced foundations. Several present hurdles contribute to making this a grand challenge. To achieve mission assurance we first need mission awareness in cyberspace. We must integrate and synchronize effects across the air, space, and cyber domains and achieve the appropriate balance and interplay between defensive and offensive cyber capabilities. We need to bolster trust in our hardware and software supply chains and find an intelligent mix of COTS and GOTS that is secure yet affordable. We must rethink the interplay of humans and cyber systems to effect better decisions more quickly. Finally, we must "change the game" to regain asymmetric advantage over attackers with systems designed with both agility and resilience.

3.2 Findings and Recommendations

3.2.1 Broaden Limited Cyber Mindset

Within the cyber domain, five findings and recommendations were developed. **The first finding is that, in the Air Force, cyber continues to be too often viewed only as an enabling capability for other domains in the sense of an "A6" staff support element.** This hampers the necessary maturation of cyber as an element of combat power in its own right. In the future, cyber operations, especially in highly contested environments, may be as much the supported as supporting activities for the conduct of Air Force missions. **This requires a change of mindset across the Air Force at all levels to properly accommodate this latest domain to be added to the Air Force mission in which we must fly and fight (OPR: AF/A3).**

3.2.2 Enhance Situational Awareness & Understanding

The next finding is that **the Air Force lacks the comprehensive cyberspace situational awareness that is a prerequisite for cyberspace assurance.** This finding has two aspects. First, in ‘blue’ cyberspace, it is presently difficult to map Air Force missions to their cyberspace dependencies even statically, much less in real-time. This is the focus of the current AF SAB study on *Cyber Situational Awareness (CSA)*. The problem will only be exacerbated when missions become agile in cyberspace. The second aspect is that awareness in neutral and hostile cyberspace is limited, and what is known often cannot be shared and fused with blue operational awareness due to classification restrictions. Fortunately, there are S&T developments that can address these findings. Specifically, **the Air Force should deliberately shape its blue cyber domain by employing proven information management techniques that would achieve mission awareness by capturing mission context in the metadata of publications and subscriptions.** This provides real-time awareness of how the mission is flowing through blue cyberspace and allows for the rapid promulgation of command and control that can adaptively tailor service delivery to mission priority within seconds based upon the commander’s intent (OPR: AFRL). The second recommendation is to build upon this enhanced blue situational awareness to increase abilities to fuse operational and intelligence information (OPR: AFSPC, OCRs: 24 AF, AF/A2). This will require developing common operational pictures, solving multi-domain security issues, and developing integrated human-machine interface capabilities.

3.2.3 Assure Missions and Protect Critical Information in Fragile Architectures

The third finding is that AF cyber architectures are static and fragile and this threatens our ability to assure missions and protect critical information from cyber attacks. The almost exclusive use of commercial devices, coupled with rather slow technology refresh gives our cyber infrastructure a broad exposure to cyber attacks from a wide community of developers that results in an asymmetric advantage over our defensive capabilities. Using components primarily engineered for functionality and low cost, rather than confronting cyber attacks results in fragile systems easily penetrated. As we envision 2025, we need to alter this asymmetric advantage we give attackers and increase the costs they incur to engineer their weapons and plan and conduct their attacks. By promoting agility and resilience to first order concerns for cyber engineering across education, S&T, and procurement, the asymmetry can be reversed. Agility should be employed at several levels, for example from IP hopping within the broad IPv6 space to processors with morphing instruction sets and applications moving amongst cloud computing environments. Similarly, resilience can be employed at many levels, i.e. from services that fight off attacks to voting multi-core architectures that act on the majority and investigate minority reports to critical software layers synthesized from layered specifications and by employing out of band techniques for command and control in contested environments **Adding agility and resilience innovations across the hardware, software, network, and application layers can turn the tables to the defender’s advantage (OPR: AFRL).**

3.2.4 Create Hardened, Trusted, Self-Healing Networks & Cyber Physical Systems

A fourth finding is that current operational and network architectures inhibit the ability to defend key mission network enclaves. In particular, the drive toward a common level of defense for all missions often leads to an affordably average solution that leaves the most critical mission networking needs wanting. While additional protections to give these missions' cyber dependencies attributes of enhanced trust and resilience might not be affordable in the large view, they warrant special attention. **The recommendation is to make key mission networks hardened, trusted, and self-healing (OPR: AFPSC, OCRs: 24 AF, MAJCOMs).** An intelligent mix of capabilities is required to deliver these enhancements at an affordable cost with arrangements to be worked out between the 24th AF and the MAJCOMs.

3.2.5 Develop Integrated and Full Spectrum Effects

A final finding is that a lack of persistent and/or dynamic access limits the operational utility and flexibility of full spectrum cyber capability. The cyber landscape is continually in flux with new devices, applications, and software updates opening and closing vulnerabilities on a daily basis. To grow the full spectrum cyber toolkit requires continual attention to these changes to stay abreast. **In addition, we found there is a need to integrate across disparate realms including cyber, SIGINT, and electronic warfare to achieve the greatest access and effects capabilities (OPR: AFSPC, OCRs: ACC, AFISRA).**

3.3 Cyber S&T Technologies

3.3.1 Assure and Empower Missions

The AF must assure successful mission execution while cyber threats are avoided, identified, contained, and/or defeated. It must have the ability to conduct effective full spectrum operations while maintaining real-time situational awareness for command and control. Achieving mission awareness in blue cyberspace is an important step toward broader cyber situational awareness. The AF must understand the dynamic, real-time mapping, and analysis of critical AF mission functions onto cyberspace including the cyber situation awareness functions of monitoring the health and status of its cyber infrastructure, and how missions flow through cyberspace. A key challenge is to develop and apply information management techniques to enable commanders to make actionable decisions based upon context and content awareness. Information management services can provide strong mechanisms that support authentication, non-repudiation, encryption, mission association, and prioritization implicit in the management of information object types. However, information management services must not overburden network performance in terms of latency or throughput penalties. The goal in this area is to support 10 gigabit flows of mission-aware information objects at TRL 6 by FY14 and then become operational at 16 AFNET points of Internet presence by FY16. The capability then scales to 100 gigabits at TRL 6 by FY17 in parallel with real-time C2 for the AFNET. In the long term, managed information becomes self-protecting which allows for the merging of segregated networks. Through the examination of commercial and other tools for cyber SA, there is little presently available at the mission level and AFRL is poised to lead this area for DoD.

Table 3.1: S&T to Assure and Empower the Mission

Area	Thread	Near (FY12-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 Gigabit Mission Aware Routing (L) 	<ul style="list-style-type: none"> • Real-time C2 for AFNET (L) • 100 Gigabit 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 Operations 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)

Development of Full-Spectrum Cyberspace Operations can provide trusted, validated, verified capabilities to deliver a full range of cyber effects to actively defend against any and all cyber threats. It requires a means to measure and assess the effectiveness and degree of assurance of a delivered cyber effect prior to usage, combining theoretical, analytical, experimental, and simulation-based approaches for quantifying cyber assets and their potential effects. A near-term challenge is to provide capability to scale up D5 (Deny, Disrupt, Degrade, Deceive & Destroy) effects far beyond present constraints. Then a broader set of capabilities must be devised by merging cyber, SIGINT, and electronic warfare techniques. In parallel with these developments, the ever changing cyber landscape requires a continual focus on devising means for access (including stealth and persistence) and effects on the latest technologies.

3.3.2 Agile Operations and Resilient Defense

Cyber warfare is like maneuver warfare, in that speed and agility matter most. In order for AF missions to avoid, fight through, and recover from attacks, AF cyber architectures must be agile and resilient at many levels. Transforming the Air Force cyber infrastructure from its current static configuration to a dynamic architecture enabling diversity will raise the level of difficulty for adversaries to conduct attacks as well as make the infrastructure more adaptive and resilient.

Resilience can be improved in several ways. First, in the near term, S&T can drive high (line) speed encryption down to a minimal cost that is acceptable to almost all applications. In the mid term, unique anti-tamper protections can be derived from nanotechnology advances including the potential for perpetually powered portions of chips that encapsulate a root of trust. Near-term work must be done to secure mobile platforms and thin out functionality that can be moved to more secure servers in cloud environments where redundancy can enhance resilience. Finally, military-grade hardware and software can be selectively mixed with COTS technology to greatly reduce vulnerability surfaces and increase the difficulty of devising successful attacks.

Table 3.2: S&T to Enhance Agility and Resilience

Area	Thread	Near (F12-FY15)	Mid (FY16-20)	Far (FY21-25)
Enhance Agility and 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 power (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)

Agility is similarly improved at several levels. Beyond present capabilities to quickly hop network IP locations, by FY 14, instruction set morphing at sub second rates will reach TRL 6 demonstration, as will agility in network configurations and routing policies. By 2017, Cyber C2 promulgation will be built upon these foundations. The emergence of cloud computing will be an important contributor to resilience and agility as well as affordability. Near term, key services will be moved to the cloud and shifted over to the use of managed information. Low level operating systems will be strengthened by applying formal methods to their construction as a key contribution to the resilience and trust of security in cloud environments. Further term, clouds afford the opportunity to move mission applications amongst a multiplicity of virtual machines to create a moving target to attackers at a layer above the traditional application layer. In much of the cloud S&T, the AF will be a fast follower and expects to highly leverage, adapt or adopt the work of others.

3.3.3 Optimize Human-Machine Systems

Through the merger of human and machine capabilities, enhanced cyber situational awareness and mission awareness can be achieved, yielding improved decision making against advanced threats and increasing AF mission success. The AF must understand and be able to measure the stress and limits the cyber domain and new cyber capabilities place on our operators. A means to enable human operators to see and operate effectively in cyberspace in relation to the physical world is necessary. The AF must develop ways to augment operator cognitive capabilities and develop their trust in automated decision processes.

Natural human capacities are becoming increasingly mismatched to data volumes, processing capabilities, and required decision speeds. Computers can keep track of many objects, but humans still remain more capable of higher-level comprehension, reasoning and anticipation. The AF must develop a common operating platform for diverse cyber missions and technology and capabilities to rapidly visualize a user defined operational picture (UDOP) from shared, common data to provide insight into complex cyber capabilities that can be readily manipulated to support AF mission-essential functions. Furthermore, complexity and rapid evolution requires AF cyber warriors to be selected based upon known critical skills and abilities, educated in the science of information assurance, and trained in the art of cyber warfare.

Table 3.3: S&T to Optimize Human-Machine Systems

Area	Thread	Near (FY12-FY15)	Mid (FY16-20)	Far (FY21-25)
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) 	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)

3.3.4 Trusted Foundations

Air Force cyber infrastructure is a heterogeneous composite of hardware and software that includes commercial off the shelf (COTS) elements, customized and militarized commercial systems, and specialized embedded systems. With the exception of a few critical systems developed and integrated in secure trusted facilities, the vast majority of the cyber infrastructure includes unverified hardware and software that is developed outside the United States. In addition to inherent security flaws, there are countless opportunities for an adversary to insert surreptitious functions.

Table 3.4: S&T for Foundations of Trust

Area	Thread	Near (FY12-FY15)	Mid (FY16-20)	Far (FY21-25)
Foundations of Trust and Assurance	Trust	<ul style="list-style-type: none"> • System decomposition and trust-worthiness 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)

Countering these vulnerabilities requires a means to gauge the level of trust in various components and to understand the risk these pose to the execution of critical mission functions. Development of technologies and procedures that address the full spectrum of supply chain concerns is needed. Technology and strategies that will enable a trusted, secure mixing of government off the shelf (GOTS) and commercial off the shelf (COTS) components throughout AF weapon systems is required. A key component to developing this trust is the ability to conduct hardware and software analysis, automated reverse engineering and development of threat avoidance metrics and modeling capabilities that will provide an understanding of the comprehensive risks in complex mission systems.

4. Air Domain

4.1 Air Domain Strategic Context

Recent technology advances in the design of aircraft and supporting infrastructure increased their functionality as well as their reliance on computer hardware, software and protocols. This reliance provided the U.S. Air Force with valuable opportunity and functionality, but it introduced vulnerabilities across the entire kill chain that may put at risk air superiority. Figure 4.1 illustrates the growth in the percentage of air platform capability dependent upon software from the F-4 (5%) to the F-35 aircraft (90%).

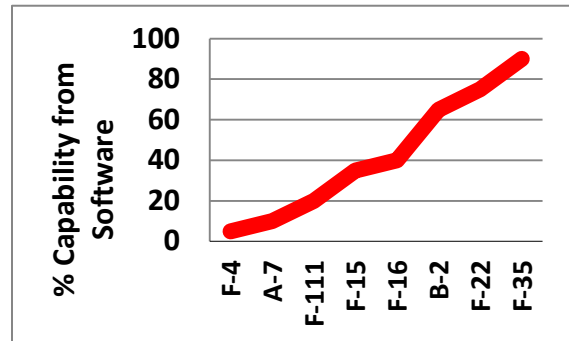


Figure 4.1: Air Platform Capability in Software (Source: SEI and LM)

To study the dependence on cyberspace of the air domain, we divide the problem into two components – the air platform and the ground support infrastructure. In turn, we divide each of these two components into two areas – aircraft vehicle systems and mission systems, and ground systems and support systems. To comprehensively consider the dependence on cyberspace of the air domain, we identified representative systems and studied their properties. Representative aircraft included the Joint Strike Fighter, MQ-9 Reaper Remotely-Piloted Aircraft (RPA), KC-46A Next generation Tanker, C-40B Distinguished Visitor (DV) transport, and C-17 Globemaster III.

For ground systems, we examined the RPA Launch and Recovery Element (LRE) and the Command and Control (C2) support infrastructure, as well as the logistics information system including Portable Maintenance Aids (PMA). While ground support systems are essential for air power, the Cyber, C2 and ISR sections of *Cyber Vision 2025* report the detailed analysis of cyber dependence of the Air Operations Center (AOC), Tanker Airlift Control Center (TACC), Distributed Control Ground Station (DCGS), and the Global Information Grid (GIG) which experience very poor cyber situational awareness.

Security

Stealth must be built into the plane. It cannot be retrofitted.

4.2.1 Design-in Security to Address Insufficient Intelligence

Finding: Intelligence on cyber threats against air platforms is not mature enough to drive requirements and S&T solutions. System Threat Assessment Reports (STAR) on air platforms and supporting infrastructures focus predominantly on kinetic threats to these systems. We found no requirement for STARs to include cyber threats into the analysis, denying the AF acquirers the benefit of specifying system requirements to meet the appropriate security needs.

Recommendation: Future acquisitions must take into consideration cyber threats and include designed-in security – layers of protection, detection, survival, and resilience – and mission assurance testing at all stages of the acquisition lifecycle (OPR: AFMC/AFLCMC, OCR: SAF/AQ). We recommend that future acquisitions formally specify weapon system requirements with designed-in security, and require formal verification that the final product satisfies the security properties

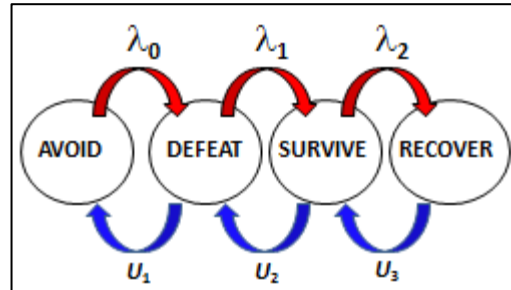


Figure 4.2:
Cyber Security Measures

of the original requirements, these recommendations are summarized in Table 4.1. By cyber security, we refer to the sum of measures aimed at (1) avoidance and prevention, (2) detection and defeat, (3) survival and fight through, and (4) resilience and recovery (Figure 4.2). We seek first and foremost to mitigate vulnerabilities and deter threats. When prevention fails, we wish to detect and react to threats before they become attacks. When detection fails, we must ensure mission survival in the presence of attacks. In anticipation of unlikely mission failure, we must build resilient systems that can recover from setback to allow us to continue the mission. The technology necessary for designed-in security and formal mission assurance is not mature and requires advancement in S&T. Consequently, developmental (DT&E) and operational (OT&E) test and evaluation of weapon systems must be conducted assuming a contested cyber environment. This study has also surfaced the need for further education on cyber systems, dependencies, risks, and vulnerabilities throughout the acquisition system.

4.2.2 Reduce Complexity and Enable Verification to Mitigate COTS Vulnerabilities

Finding: The heavy reliance on Commercial off the Shelf (COTS) products in acquisition trades security for cost and speed, raises concerns on supply chain trust, and introduces potential cyber vulnerabilities in air vehicles and ground support platforms. General Atomics built the MQ-1 Predator as a technology demonstration and focused on speed of delivery of the product. In the process, security considerations were not addressed. As RPAs evolved from experimental surveillance aircraft to weapon platforms, the security requirements and protections against cyber threats did not evolve correspondingly. Similarly, Lockheed Martin adopted COTS hardware and software in the JSF for their proven reliability, resulting potentially in security vulnerabilities in the air vehicle and the ground logistics support infrastructure.



Figure 4.3: Aircraft Maintainers with COTS Plug-In Devices

Recommendation: To capitalize on the benefits of COTS components, the USAF must reduce the complexity of future requirements of air platforms while improving the clarity and importance of cyber requirements to permit formal verification of security properties

(OPR: MAJCOMs, AFLCMC). It is important that the AF understands how complexity drives S&T requirements. The state-of-the-art allows formal verification of computer programs up to 1 million lines of code, such as the formal verification of separation kernels on air platforms. These can then serve as trusted building blocks in composable systems. Reducing the complexity in the specification of future requirements achieves the dual benefit of reducing vulnerability while allowing formal verification of additional system components.



Figure 4.4:
B-2 Crash in Guam

4.2.3 Secure Full Life Cycle to Overcome Insufficient Security Architectures

Finding: Technology solutions and processes, including root of trust and cryptography, exist today to address many vulnerability concerns, but point solutions do not make up for a limited overarching security architecture. The absence of a security architecture in the acquisition requirements of weapon systems results in complex systems with ineffective point solutions such as firewalls and intrusion detection systems. Although the formally-verified Green Hills Integrity separation kernel and the custom-designed Field Programmable Gate Array (FPGA) Network Interface Units (NIU) are positive examples of effective point solutions on the JSF, they may not necessarily assure air platform missions against potential vulnerability elsewhere in the architecture.

Recommendation: The USAF must extend security solutions into a security architecture in which technology fixes must “buy their way” onto systems. Recapitalization of cyber systems on legacy platforms must be taken into account and folded into acquisition / sustainment strategies (OPR: AFMC/AFLCMC, MAJCOMs, AFMC/FM). The wide disparity in cyber protections among legacy platforms increases the complexity of implementing uniform security measures. Distinguished Visitor (DV) transport and the Air Operations Centers (AOC) are examples of systems with large numbers of different configurations. We require capabilities to patch COTS-based components and antiquated systems in a cost-effective and timely fashion.



Figure 4.5:
DV Aircraft

4.2.4 Secure Platform IT to Mitigate Outdated Security Policies and Controls

Finding: Cyber security policies and IA controls have not kept pace with complexity of weapon systems. Extending office automation security policies, Tactics, Techniques, and Procedures (TTPs), and Certification and Accreditation (C&A) onto weapon systems, or worse yet isolating weapon systems even from the basic security controls of office automation, fails to assure critical missions in a contested cyber environment. The DoD Information Assurance Certification and



Figure 4.6: RPA
Crash in Sychelles

Accreditation Process (DIACAP) proved ineffective and potentially detrimental for mission assurance – a software developer may forego fixing vulnerabilities to avoid repeating an onerous C&A process – and is neither necessary nor sufficient for assuring air vehicles against cyber threats. We recognize that DoD is in the process of adopting a security approach for platform IT, which will include weapon systems. While the current DoDI 8500.2 exempts weapon systems from IT certification and accreditation processes and standards, DoD will soon publish security standards to assure mission success for platform IT with the re-issuance of 8500.2.

Recommendation: Platform IT security requirements must exceed those for office automation (OPR: AFMC, SAF/CIO A6). We recommend strengthening the security requirements for Platform Information Technology (PIT) systems to exceed those of business office automation IT by shifting the emphasis from detection to prevention, from network defense to mission assurance, and from manual response to autonomous mission survival.

4.2.5 Secure C2 Architecture to Address Brittleness

Finding: The current command and control architecture is a key detriment to remotely piloted operations. The C2 architecture for remotely-piloted operations has proven problematic in terms of latency and vulnerability, and may offer a sophisticated adversary an attack vector against RPAs. Brittle C2 is also problematic in other air systems.

Recommendation: Invest in S&T solutions to revamp C2 architecture (OPR: AFRL, AFMC/AFLCMC). We recommend a clean-slate approach to the C2 architecture for RPAs that will result in a formally-specified architecture whose security properties can be verified as the next logical step towards fully-autonomous air operations.

4.2.6 Overcome Insufficient Cyberspace Situational Awareness

Finding: Operators in air platforms and C2 centers lack real-time awareness of mission dependence on cyberspace. The heavy utilization of commercial communications infrastructure denies operators timely awareness of the dependence of their missions on cyberspace, the impact of a cyber attack on integrity, and attribution to agents or natural causes.

Recommendation: Focus on technical solution sets that allow “fighting through” cyber attacks (OPR: AFMC/AFLCMC, AFRL). Develop related cyber curricula for air domain operators throughout professional training and education (OPR: AETC, MAJCOMs). The USAF should incorporate cyber curricula throughout the professional education of pilots, navigators, testers, ground operators, and maintainers, including the Undergraduate Pilot Training and the Test Pilot School, with an emphasis on mission assurance and fight through cyber attacks.




4.3 Science and Technology Solutions

Table 4.1 captures the near-, mid-, and far-term cyber S&T investments necessary to reduce risks and increase benefits of air systems having considered vulnerability, projected adversary

capability, and estimated consequences of a successful attack. The matrix delineates core cyber systems within air vehicles, mission systems (e.g., sensors, communication, air traffic control), ground and support systems (e.g., launch and recover elements, air operations centers).

Table 4.1: Air Domain S&T Recommendations

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

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

The top S&T areas where the USAF must lead to achieve the greatest impact on assuring the Air Superiority Core Function in a 2025 contested cyber environment include (OPRs: AFSPC, ACC, AFRL):

4.3.1 Anti-Tamper Root-of-Trust (L)

The Air Force will lead in this area with the need driven by unmanned systems and ever smaller field computing and communication devices. Our ability to remotely control unmanned systems

over great distances leaves open the possibility of loss of those systems to our adversaries. The development of anti-tamper technologies ensures that if those systems fall into the wrong hands, the ability to reverse engineer those systems will be minimal.

4.3.2 Cyber Black Box (L)

Many avionics systems assume built-in trust, despite supply chain concerns and system complexity flaws. As our platforms become more richly connected to outside networks and data sources, the eventuality of untrusted activity on our platforms becomes more likely. We require technologies that aid in the modeling of and reasoning about complex software and hardware systems, and collecting real-time data that can help determine if and how systems are under cyber attack. This activity is akin to the ‘black box’ on aircraft that can not only reconstruct if/when unexpected events have occurred, but also act as a state-based aircraft bus message guardable to quantify good behavior and prevent the exchange of data or the execution of software outside these norms.

4.3.3 Secure Maintenance Aids (L)

The Air Force has seized the opportunity for ease of maintenance through the use of COTS hardware as portable maintenance aids. While the use of COTS is cost effective, the cyber and physical security properties of these devices must be proven to minimize the attack vector that they introduce. TTPs should be examined to compute the risk for each maintenance aid.

4.3.4 GPS Hardening and Alternatives (L)

The Air Force depends on GPS for precision in mission execution. Hardening the system against threats both on and off aircraft will continue to be led by the Air Force. For GPS alternatives, this activity will provide alternative methods for deriving that precision in the absence of the GPS constellation. It will be measured against the precision derived by the GPS system and compared to the resolution needs of the weapon systems that depend on it.

4.3.5 Collaborative/Cooperative Control (L)

The Air Force will lead in developing the ability for unmanned air vehicles to cooperate on missions with little or no human intervention. Developments in autonomy and airborne mobile ad hoc networks will be key to the success of this area. Success will be demonstrated when C2 operators can direct a group of platforms on ‘what’ needs to be done and the platforms determine ‘how’ that will be carried out.

4.3.6 Advanced Satellite Communications (L)

Our use of satellite communications to support airborne ISR missions is critical. Moving into the V/W frequency bands allows us to support higher bandwidth links and tighter beams which improves our overall resistance to jamming. Measures of throughput and overall global availability will be indicators of success. The Air Force will continue to lead in this area and expects industry participation to increase in the coming years.

4.3.7 Managed Information Objects (L)

The Air Force will lead in developing a new method of managing information based on information objects. Each object will contain metadata and payload information and the metadata will include security information, information priority, mission dependence, etc allowing the infrastructure to route and transmit accordingly. Success will be measured by our ability to assure mission execution through delivery of all required information in a timely manner.

4.3.8 Trusted Cloud Computing (L)

Cloud computing offers great opportunity for data distribution, replication etc. and is largely commercially driven. The Air Force will leverage this enormous commercial investment and lead only those activities that are specific to Air Force mission needs with respect to increased security, and privatization.

4.3.9 Mission Mapping (L)

The Air Force's ability to guarantee Mission Assurance is dependent on our understanding of the cyber dependencies of those missions. This activity is being led by the Air Force to map those dependencies to the point where we can autonomously understand those dependencies and protect them accordingly.

4.3.10 5th to 5th Platform Communications (L)

The Air Force has a critical need for interoperability among its 5th generation air platforms. The trade between data sharing for combat effectiveness and maintaining stealth is a key challenge in this area. Leadership in this S&T underpins our ability to gain/maintain air superiority.

4.4 Conclusions of Air Domain

The dependence on cyberspace of the USAF Air missions is significant and will increase over the next decade. Software functionality on aircraft has increased dramatically from the F-4 to the F-35, providing unsurpassed capabilities and introducing potentially exploitable cyber vulnerability.

We found that intelligence on cyber threats against air platforms was not mature enough to drive requirements and S&T solutions, and the heavy reliance on COTS in acquisition trades security for cost and speed, raises concerns on supply chain trust, and introduces potential cyber vulnerabilities in air vehicles and ground support platforms. Technology solutions and processes, including root of trust and cryptography, exist today to address many vulnerability concerns, but point solutions do not make-up for limited overarching security architecture, while cyber security policies and IA controls have not kept pace with complexity of weapon systems. The current command and control architecture is a key detriment to remotely piloted operations. Operators in air platforms and C2 centers lack real-time awareness of mission dependence on cyberspace.

We recommend that future acquisitions must include designed-in security and mission assurance testing at all stages of the acquisition lifecycle, and the USAF must reduce the complexity of future requirements of air platforms while improving the clarity and importance of cyber requirements to permit formal verification of security properties. Technology fixes must “buy their way” onto systems. Recapitalization of cyber systems on legacy platforms must be taken into account and folded into acquisition and sustainment strategies, and platform IT security requirements must exceed those for office automation. We recommend investment in S&T solutions to revamp C2 architecture, a focus on technical solution sets that allow “fighting through” cyber attacks, and the development of cyber curricula for air domain operators throughout professional training and education.

5. Space

5.1 Space Domain Strategic Context

Ever since the Desert Storm war, it has been clear that the U.S. possesses an imposing space presence. Adversaries have recognized this and now view U.S. space capabilities as a threat. The result is that some hope to asymmetrically negate our space capability by exploiting U.S. vulnerabilities. In fact, adversaries could do more than affect us militarily by negating space assets, since much of our economic prosperity depends on space.

There are several aspects to the current U.S. Space Superiority. For example, our space capabilities have made it possible to conduct high precision navigation, enabled by GPS. This has given the U.S. military unprecedented capability to field highly-precise weapons, which has the effect of reducing collateral damage as well as inflicting surgical-like damage on the adversary. Similarly, secure and survivable communication enabled by MILSATCOM allows for assured nuclear command and control, as well as expanding a commander’s ability to direct assured operations, and allowing warfighters to communicate in the most hostile environments. Cyber and communications capabilities extended world-wide allow for remote operations of Remotely Piloted Vehicles, and fuse air, space, and cyber capabilities to conduct real-time operations across the world. Missile warning from space provides near real-time knowledge of hostile missile launches. Because of these facts, some countries are re-inventing their own space technologies such as GPS for their own uses, to ensure their access to GPS-capabilities if they perceive the U.S. will ever deny them use, or if they might lose access via GPS-denial technologies of their own.

All of these capabilities depend on cyber and that dependency is growing as shown in Figure 5.1. And as good as our space systems might be, our satellites, launch enterprise (launch ranges and launch vehicles), ground infrastructure, and associated terminals are all just cyber nodes on a grand network and are vulnerable to exploitation. For example, some have claimed in open

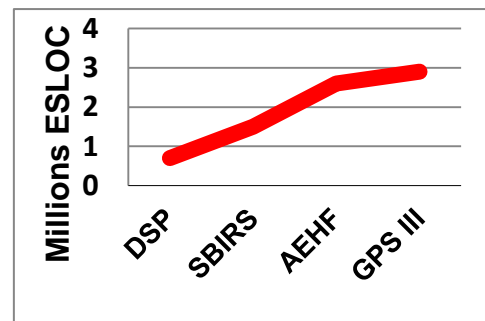


Figure 5.1: Space Systems Software Growth (Source: SEI)

forums that they can take control of our satellites through the Command and Control (C2) links. In fact, a case can be made that the currently most vulnerable portions of our space enterprise reside on the ground, probably in these C2 links. These and other cyber vulnerabilities menace our warfighting infrastructure, and allow small, non-linear threats – such as a computer virus, false data (spoofing), or foreign insertions in our supply chain – to effectively negate trillions of dollars of defense investment, and perhaps even circumvent our national capability. To prevent this, we will need to secure the ground infrastructure and terminals today.

Our networks are continuously under cyber attack. Adding to the problem is that there are supply-chain concerns for our space-based, launch, and ground infrastructure. Furthermore, cyber nodes may be accessible by non-traditional means; and there is a finite probability that insider threats may exist. This greatly expands the threat window that may compromise our national security. And the threat has grown to embrace traditionally “safe” equipment, developed and built in the U.S. For example, as the USAF begins to use a broader range of launch vehicles (Falcon, Taurus, Minotaur, etc.) that are commercial or more commercial-like, the cyber vulnerabilities of those launch vehicles represent a significant challenge as well. The salient factors are the current costs of launch and the space architecture extant, including a strong reliance on radio frequency (RF) communications to provide the capabilities noted above. We expect the trends to continue, barring revolutionary changes in space launch costs. That is, the USAF will probably rely more and more on commercial providers, and so we require a strategy to protect the information passing through those providers.

The problem we need to address for the space domain with respect to cyber activities is to protect both ground- and space-based assets that provide space services, ranging from the supply chain to the conduct of integrated space, air and cyber operations. In fact, the cost of current space systems causes a long acquisition cycle, so that space assets are expensive and take a long time to produce. In contrast, the threats to our space systems are here even today. Therefore, we must move quickly.

But the good news is that just as these space cyber nodes are rendered vulnerable, they are also open to known and proven techniques for mitigating these threats.

5.2 Findings and Recommendations

5.2.1 Develop a Resilient Architecture to Address Space Network Vulnerabilities

Finding: For the space domain, we first recognize that satellites, launch, ground infrastructure and terminals are all essentially just nodes on a grand network, and that they are vulnerable. Thus, we need to have an integrated air-space-cyber effects package that can defend against our own vulnerabilities while delving into adversary domains.

Recommendation: The overarching recommendation for mitigating the fact that our satellites, launch, ground stations and associated terminals are cyber nodes on a network is to develop an integrated, resilient, and disaggregated space, launch, and ground

architecture that will be robust to cyber as well as other threats such as ASATs (OPR: AFSPC/A8/9). The OPR for this recommendation may be enabled by implementing several technological strategies.

The National Security Space community has come to recognize the extent to which we are dependent on small numbers of high-value satellites, and has therefore embarked on a path to augment legacy space systems (Communications, Missile Warning, GPS, and Space Situational Awareness) with smaller, fractionated, disaggregated, reconfigurable, and networked systems. Moving away from integrating many capabilities on a single large platform to proving less capability on more, smaller platforms effectively increases the number of “targets” that an adversary must overcome, and thus reduces the vulnerability of the overall system. (Note: it is true that the number of attack “vectors” or nodes may increase as we fractionate satellite architectures, but the overall vulnerability of the space service under attack is in principle reduced.) We have to be careful here. Fractionating the space capability without providing diversity in functions may not decrease the vulnerability much, since if the adversaries can get to one satellite service through cyber, they can get to any copy of it. So we should ensure that the system architecture provides sufficient diversity to increase the “cost” to any attack. Fractionating, or dividing up the system, also demands that a robust, networked communications interface be established among the fractionated functions – but also results in the ability to add more capability “at the margin” by inserting additional capability when needed. This helps ensure the system is kept up-to-date with additional hardware, or even by replacing hardware if necessary. In addition, the ability to reconfigure – to autonomously change from one function to another – helps overcome obsolescence and allows the system to respond to new threats that may not have been important or present when the system was first designed. Finally, such a system is more robust to the loss of individual nodes; it will degrade gracefully. The OPR for this recommendation is AFSPC/SMC.

Second, intelligently mix GOTS and COTS to mitigate cyber vulnerabilities (OPR AFSPC/SMC). The issue is not open versus closed systems, but rather to leverage the work being accomplished by dozens or even hundreds of collaborators, and applying those best practices to GOTS. We are moving toward the disaggregated space architecture, but we are also increasingly moving toward commercially hosted payloads and commercial space services. Therefore, we will need to assess the current military and commercial system vulnerability to cyber threats, including future cyber threats, and introduce appropriate cyber mitigations.

Third, develop and deploy technologies such as flexible and scalable encryption for reconfigurable sensors and fractionated platforms that will allow the operator to fight through adversarial attack. (OPR: AFSPC/SMC/AFRL). The ability to reconfigure “on the fly” married with advanced secure communications, such as quantum key distribution and quantum cryptography, allow operators to mitigate current threats, with the goal of moving to a capability to be able to anticipate the threat and reconfigure before the threat occurs. However, we should understand that in battle, there will almost inevitably be losses of some space

services. The fractionated architecture will help with its graceful degradation, but we will also need to be able to rapidly replenish the space architecture in the event of a loss of service. The point is that a resilient system that contains redundancy as well as diversity in functions can provide the U.S. a robust space capability into the indefinite future.

5.2.2 Enhance Space Anomaly Detection and Attack Attribution

Finding: It is difficult to distinguish among space environmental, system, or adversary-induced effects. Some suggest in the open that they can control U.S. satellites via cyber attacks in the C2 links. In fact, there have been some successful cyber attacks in the last few years, as exemplified in Figure 5.2. These attacks were against the ground infrastructure and C2 links, not against satellites per se. But we expect that future attacks could also involve our direct space assets, which operate in the hostile space environment. Currently, we would not necessarily know when this occurs, as we have few methods for distinguishing natural C2 anomalies (such as from space environmental effects, or internal component or system failure) from hostile attacks. In short, we have insufficient space situational awareness.

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—**Landset 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—**Landset 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



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

Figure 5.2: Successful Space Cyber Intrusions

Recommendation: Mitigate poor space situational awareness by developing better technology for effectively modeling and reasoning about our onboard space systems along with installing high fidelity instrumentation onboard satellites that enable them to distinguish between anomalies caused by adversaries and those caused by environmental effects. (OPR: AFSPC/SMC/AFRL). Exploiting the technologies listed below in Table 5.1 can make our satellite systems more robust to attacks.

5.3 Space S&T Recommendations

Table 5.1 summarizes our S&T recommendations related to the space cyber arena using the four central focus areas that cut across Cyber Vision 2025: “Assure and Empower the Mission,” “Optimize Human-Machine Systems,” “Enhance Agility and Resilience”, and “Foundations of Trust and Assurance”. The OPR for this recommendation is AFSPC and AFRL. Table 5.1 focuses on a few important technologies where the USAF can lead, follow, or watch in the space-cyber arena in order to make our satellite systems more robust to successful attacks.

Table 5.1: Space Domain S&T Recommendations
Technology Leader (L), Follower (F), Watcher (W)

Area	Near (FY12-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 communications 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 generators that produce software that is correct by construction (W)

5.3.1 Near Term: Cyber Test Beds, Space Sensors, Reconfigurable Antennas, Trusted Foundries

In the near term, the USAF should lead in the development of space/cyber test beds to demonstrate fractionated, fight- and operate-through systems that can quickly insert technology advances into operational systems. This is responsive to the first space finding and recommendation, and would permit us to test whether the increased number of attack vectors in a fractionated architecture can be tolerated as the space system continues to provide the services that guarantee U.S. space superiority today. The AF should also lead in the development of

space environmental sensors and satellite cyber sensors that can identify and attribute anomalies in real-time. This is responsive to the second space recommendation, and will permit the U.S. to rapidly ascertain whether malfunctions are due to the space environment, subsystem failures, or hostile attacks.

Also in the near term there is a need to restructure cyber acquisition and operations policy to enable this rapid and full spectrum insertion of new technologies. While this is neither a space-specific nor an S&T activity, it is critical to implementing S&T solutions in the near term. Technologies such as reconfigurable antennas and algorithms will enhance agility and add to the resilience of space systems, but these and other advancements must be quickly adopted. When employing new technologies, the AF should continue to watch the development of foundations of trust – hardware foundries and trusted software generation – that need to be established to assure trusted capability.

5.3.2 Mid Term: Survivable C3, Malware Detection, Autonomous Self-healing Systems, Trusted Architectures

In the mid term, the AF should develop and implement entirely new technologies that permit us to ensure that we can continue to provide the critical space missions that are central to our warfighting capability: Communications, Position/Navigation/Timing, Missile Warning, and Space Situational Awareness. To that end, the AF should lead in the development of survivable, assured, real-time C3 capability in the theater. An example of this is Software Defined Radio (SDR), where we can access the communications equipment while a satellite is on orbit and change fundamental operating characteristics in response to a perceived threat. Similarly, technologies that can provide the capability to detect hidden functions and malware in our integrated space/cyber/air systems through the use of hypervisors should be exploited. A hypervisor is a supervisor over the execution of multiple operating systems that share common hardware. Every space service should be able to leverage this capability. It should include the ability to perform autonomous self-healing in the event of an attack.

Also in the mid term, the AF should lead in generating trusted satellite-cyber architectures and strong authentication for C2. We already know the threat is there, as we have discussed above, so it is time to implement technology solutions to prevent any imposition on our C2. As part of this, we may require advanced communications approaches such as laser communications to enhance assurance. For example, technologies that are emerging from academia and industry to demonstrate the generation and detection of single photons with high quantum efficiency will enable these architectures. And far-term capabilities such as quantum key distribution (QKD) are dependent on these technologies to enable flexible, scalable high-rate encryption that cannot be hacked.

5.3.3 Far Term: Verified Code Generation, Intent Detection, Cognitive Communications, Space Quantum Key Distribution

In the far term, the AF should watch the development of some technologies, such as autocode generators that produce software that is correct by construction. Such a technology might greatly simplify the currently very expensive software generation aspect of space acquisitions, while simultaneously providing robust cyber protection. Similarly, we should follow the development of technologies such as tools for intent and behavior determination to optimize human-machine systems. That is, we need to understand what adversaries are trying to do to our space systems, even as we rely more and more on autonomous, trusted software. We then have a chance to design responses to either defensively or proactively protect those critical space services.

To enhance agility and resilience in the far term, the AF should lead the development of cognitive communications for agile, reconfigurable, and composable communications and sensors. That is, we must go beyond SDR to actually sense the environment in which we operate and change procedures autonomously based on the information. In addition, the AF should step up to lead the far-term development of small, networked satellite constellations for communications, GPS and missile warning. Again, this is perhaps the most important activity we can undertake to provide a robust space architecture, and it is responsive to the first space recommendation.

As addressed further in the mission support section of this report, we will also need to lead in the development of the next generation of cyber savvy space warriors. We must attract, recruit, motivate, train, inspire, and retain the brightest who can master the complex intellectual challenges faced in the space cyber domain. This is particularly important in the space domain because of our broad mission dependence on space and because of the unique aspects of space including the high cost to build, high cost to launch, high natural threat environment, and lack of an ability to easily repair things. Collectively this places a premium on cyber assurance and resilience across the ground and space architecture.

Finally, while advanced technologies are needed to make space robust to cyber attack, the Air Force should perform a “Follow” role or a “Watch” role in areas such as policy (where we are not historically the lead), foundations of trust, and some hardware systems.

6. C2 and ISR

6.1 C2 and ISR Strategic Context

The Air Force’s ability to command and control (C2) airpower, and maintain an information advantage with actionable intelligence, surveillance and reconnaissance (ISR) products is a strategic advantage demonstrated repeatedly on the world stage since Operation DESERT STORM. From the opening phases of Operation IRAQI FREEDOM, when the JSTARS Ground Moving Target Indicator targeted Iraqi armor during a complete brownout, to the countless

hours of full motion video used to silently track objects during the past 10 years of counter-insurgency operations in Operation ENDURING FREEDOM, the battlefield effects have been undeniable.

Potential adversaries have taken notice; articles have been written in a myriad of languages discussing and dissecting the U.S. asymmetric advantage. C2 and ISR is unquestionably a U.S. strategic center of gravity. The cost to attack that center of gravity becomes lower and lower as malware becomes an Internet-accessible commodity. Our networks have already been probed, enumerated, infiltrated, implanted, and disrupted. In a contested cyber environment, the AF's ability to maintain its strategic C2 and ISR advantage will depend on mitigating cyber vulnerabilities in the C2 and ISR support infrastructure, and its resilience to cyber attack and agility in the face of adversary cyber maneuver.

6.2 Findings and Recommendations

6.2.1 Focus Teams of Experts to Assure Contested C2 and ISR

Finding: The U.S. created its C2 and ISR advantage by leveraging the cyber domain from its inception; in an increasingly contested cyber domain, that advantage is at risk. The classified examples studied by the C2 and ISR team make it clear that our C2 and ISR systems have cyber vulnerabilities, some that can be triggered spontaneously simply by physical stimuli or unintended misuse, and others that a persistent adversary is able to ascertain and exploit purposely. The inherent security in legacy systems or the designed-in security of newer systems can be degraded or lost as system enhancements and upgrades create cyber attack vectors. Unchanging systems are also at risk, as the patient and persistent sophisticated cyber adversaries can learn more about a C2 and ISR platform through constant surveillance over the lifespan of the system.

The complexity of most systems in conjunction with the absence of a security architecture and the resulting vulnerabilities allows threats to lay dormant for extended periods of time, buried deep within multiple interface or integration points to be exploited at specific times or events in the future. In a given C2 and ISR system, it is highly likely that some adversary has already exploited one or more vulnerabilities and has a cyber attack capability ready to launch at the time of his choosing, against a platform, its communications and data links, the integrity of the information received, or even its support and maintenance. Under these circumstances, the U.S. may not only lose its C2 and ISR advantage, but without preparation for "fighting through" and restoration, the U.S. may suffer a disastrous disadvantage.

Recommendation: Focus teams of mission specialists, system architects, and cyber experts on assuring critical mission threads (OPR: AFSPC). The USAF already deploys highly skilled hunter teams to conduct deep cyber operations. These teams, augmented with users, system architects and cyber defenders, could turn an intense spotlight on system vulnerabilities that can be exploited to cause Blue C2 and ISR mission failure. Unlike Red Teams, who look

for “ways in”, these teams will look for the full attack path that must be followed by the adversary. The cyber defenders can determine network or enterprise configurations to block or mask the path at its weakest point, at a minimum increasing the cost or risk to an adversary. System architects can weed out vulnerabilities in the normal operations and maintenance cycle. As these new teams conduct their operations, the S&T community can capture their output and maintain a mission assurance framework for future use, continuously raising the bar for even sophisticated adversaries.

6.2.2 Create Intelligent Processing Capability to Overcome Massive Data Deluge

Finding: The amount of data collected by our ISR and Cyber sensor systems exceeds our capacity to discover, analyze, produce and disseminate meaningful and actionable information to support timely decision making. While decisions improve with more accurate situational awareness (SA) supported by an underlying rich data set, these same decisions can be degraded in an environment where the sheer amount of data effectively masks the actionable information and thus effectively inhibiting timely and accurate decision making. The amount and diversity of data collected by our traditional ISR sensors and open sources across air, space, and cyberspace domains has been exploding (e.g., Full Motion Video (FMV), Wide Area Motion Imagery (WAMI), hyperspectral, signals intelligence, LIDAR). Before our ability to collect data can improve our C2 capability, significant investment in the ability to perform automated discovery and machine-based analysis, effectively reducing the data into actionable intelligence, and automated dissemination is needed.

This issue is particularly acute in the realm of cyber defense sensors (e.g., Host Based Security System (HBSS) and Information Operations Platform (IOP)). In addition to the previously discussed ISR Sensors, cyber sensors today collect petabytes (10^{15} bytes) of data, and in the near future will surpass yottabytes (10^{24} bytes). Beyond the elementary storage and bandwidth requirements of big/large data, the cyber ISR enterprise is ill equipped to discover, analyze and produce against large data sets in tactically useful timeframes to support decision makers and automatic response systems.

Recommendation: Create new massive data processing capability (OPR: AFMC/AFLCMC, AFPSC). To turn the increasing capabilities of sensor systems into superior C2 and ISR systems, new approaches must be created, including moving processing closer to the sensor and developing context aware capabilities to reduce the analysis surface. The scope of the solution space must address the following key areas: (1) minimize the data required off the platform; (2) transport only essential data across the network; (3) efficient storage of and access to the data; and (4) automated intelligent analysis of the data. The commercial sector of the economy, especially healthcare,



retail and manufacturing are making large investments in large data for competitive advantage in the market place. The Air Force must monitor and leverage to the maximum extent possible investments in technology made by commercial industry and other governmental partners.

Beyond managing large data sets, cyber C2 and ISR also requires the development of algorithms and visualizations capabilities to make activities in the cyber domain intelligible to human decision-makers. Commercial entities, such as large Internet Service Providers (ISPs), are making investments in cyber situational awareness, but these efforts fall short of military C2 and ISR requirements.

6.2.3 Assure Information Integrity of Cyber-enabled C2 and ISR at the Tactical Edge

Finding: While digital collaboration between the enterprise and the tactical edge increases situation awareness and ops tempo, it also increases exposure of C2 and ISR systems to cyber attack and operators to externally generated, maliciously altered, non-authoritative or non-attributable data. Recent warfare in Iraq and Afghanistan, with its emphasis on defeating insurgents, has expanded the role of the Joint Terminal Attack Controller (JTAC) and the systems needed to defend troops in contact with the enemy. Small form factor computing devices such as ruggedized laptops and video receivers are now commonplace to support digital C2 for close air support and increase SA at the lowest tactical echelons. Tactical platforms can now potentially be exploited over digital networks, and the Combined Air Operations Center (CAOC) is now reachable from radios and digital devices in the field that could fall into enemy hands.

In addition, C2 and ISR systems and operators are exposed to externally generated content that increases the risk of processing maliciously altered, non-authoritative or non-attributable data. Unlike a denial of service, which is immediately obvious even if detrimental, a failure of integrity can have disastrous consequences before it is even noticed. For example, an F-16 pilot who gets a bad coordinate for a target (say the locations of the target and the JTAC have been reversed in the digital 9-line) may or may not prosecute that target depending upon contextual information he may have.

Recommendation: Develop the Means to Assure Information Integrity

Effective use of tactical cyber C2 and ISR requires a means for establishing provenance and assuring integrity as information is generated and traverses the enterprise and tactical networks (OPR: AFRL). Emerging concepts for tactical networks such as the Joint Aerial Layer Network provide a degree of confidentiality and availability, but they do not address data integrity. The AF must develop affordable means to safeguard and verify the integrity of individual messages while still providing a robust tactical network that is compatible with existing TTPs; that is, that operate robustly and support extended mission timelines without reachback. Technologies such as guards, multiple independent levels of security, advanced bus controllers, digital watermarking, and advanced embedded processors

could help reduce vulnerability to attacks on data integrity, but the AF must tailor the information content and protections to the tactical environment where bandwidth and reachback may be limited. Managed Information Objects (MIOs) that encapsulate both information content and context have been demonstrated to improve the efficiency of cross-domain guards; however, the AF should increase its nascent research into self-managing information objects that offer the potential to eliminate guards altogether through context-sensitive selective disclosure and/or self destruction.

6.2.4 Mature Cross Domain Synchronization

Finding: Synchronizing air, space, and cyber (A/S/C) assets to maximize effects and leverage non-traditional ISR are nascent concepts. The current C2 and ISR enterprise is composed of individual worldwide entities or nodes, some servicing a specific domain, that collectively provide the full range of C2 and ISR capabilities on a global scale. C2 and ISR capabilities are not currently organized, manned, or equipped sufficiently to coordinate air, space, and cyber assets seamlessly across the entire range of military operations within each domain to achieve desired effects.

Recommendation: Develop C2 and ISR using world-wide, distributed nodes synchronized and integrated across air, space, and cyber operations employing all assets in the most effective manner (OPR: AFRL, AFISRA). Future C2 and ISR requires world-wide, distributed nodes seamlessly synchronized / integrated across disparate air, space, and cyber operations, employing all assets in the most effective manner. The envisioned capability includes: 1) rapid generation and assessment of kinetic and non-kinetic courses of action; 2) integration of all forces within the battlespace in both virtual position and time to achieve the desired effects; 3) kinetic/non-kinetic analysis and assessment for the attainment of complex effects at all levels of the campaign and 4) institutional acknowledgement of cyber network exploitation techniques, as well as cyber intelligence of and in open source, signals, communications, electronics, movement, steganography, and voice and video services as core ISR missions; and the exploration of some cyber assets as additional forms of non-traditional ISR.

6.4 C2 and ISR S&T

Protecting, and even increasing, the C2 and ISR advantage will require many advances in S&T. In most areas, some research already exists; in all, new S&T must be pursued vigorously to keep pace with the growing threat.

6.4.1 Assure and Empower the Mission

Today's cyber-enabled C2 and ISR empowers the AF's missions in its traditional domains of air and space; however, as the U.S. freedom of action in cyberspace is increasingly contested, cyber itself has become a warfighting domain. Assuring and empowering traditional C2 and ISR requires a new cyber C2 and ISR capability. This capability must be based on a quantitative understanding of the effectiveness of cyber assets. Beyond empowering the C2 and ISR

mission, the obvious utility of cyber power to create far-reaching effects requires the AF to make it part of its war-fighting arsenal. To empower the overarching AF mission, cyber effects must be integrated with air and space effects to create an optimally effective plan. Most of the core science and technology needed for this capability is yet to be conceived or developed. The S&T goals for this area are shown in Table 6.1.

Table 6.1: Assuring and Empowering Cyber C2 and ISR

Area	Near (FY12-FY15)	Mid (FY16-20)	Far (FY21-25)
Assure and Empower the Mission	<ul style="list-style-type: none"> • Semi-automated Cyber-Mission Mapping (L) • Integrated Physical-space and Cyber-space M&S (L) • Cyber asset characterization (F) • New Data Compression (F) 	<ul style="list-style-type: none"> • Automated Cyber-Mission Mapping (F) • Validated Physical-Cyber Space Models Integrated with Test Beds (L/F) • Large scale cyber quantification and effects estimation (L) 	<ul style="list-style-type: none"> • Dynamically Generated Cyber-Mission Mapping (L) • Fully Integrated Capability to Predict Cyber Effects on Mission Systems (F)

Interestingly, some of the required S&T is applicable to both cyber defense and offense. Both require the capability to map mission essential functions (MEFs) to cyber assets. It is exceedingly difficult to trace and disambiguate the processing and network traffic specific to a mission as it traverses a network. In the near term, intense research in this area may result in a semi-automated capability to perform mission-to-cyber mapping; in the mid term, a completely automated capability for relatively static networks; and in the far term, a capability to map networks as they change dynamically. Red mission-to-cyber mapping is and will remain largely a function of intelligence-gathering; however, the same tools developed for mapping Blue missions, may guide data collection for mapping Red missions.

Mission-to-cyber mapping enables prediction and quantification of cyber effects on Mission Measures of Effectiveness (MOEs) using traditional testing and Modeling and Simulation (M&S) approaches. Advances in faster-than-real-time, validated cyber models and integrated physical space force-on-force models (e.g., a sortie in contested air space) are required. Significant advances in cyber testing and test ranges are required to increase test fidelity and turnaround timelines. Accurately characterizing the effect of a cyber asset gives planners and commanders the ability to make optimized decisions. In the near term, physical-space and cyberspace models can be integrated based on the rudimentary near-term mission-to-cyber mapping; in the mid term, real-time or better M&S should be merged with high-fidelity results from test ranges and exercises for confident prediction of both cyber defensive and offensive effects; in the far term, real-time decision support that merges theoretical, analytical, experimental and simulation-based approaches for cyber asset analysis and assignment will allow agile responses to changing conditions in real-time. Successfully exploiting these technologies will enable cyber assets to be tasked on par with their air and space counterparts.

6.4.2 Optimize Human-Machine Systems

S&T advances in the realm of Human-Machine Interfaces (HMIs) are needed to create a cyber C2 and ISR capability with deeper and more meaningful situational awareness and more responsive integrated autonomous/human-in-the-loop C2. Cyber-mission mapping and cyber asset characterization will be essential elements in creating both HMI capabilities. In the case of Cyber SA, the AF must also develop basic concepts and fundamental cyber principles. These goals are summarized in Table 6.2.

Table 6.2: Human-Machine Systems

Area	Near (F12-FY15)	Mid (FY16-20)	Far (FY21-25)
Human-Machine Systems	<ul style="list-style-type: none"> • Visualization of cyber impacts on missions (L) • Autonomic responses to reliable indicators of adversary activity (F) • Validated framework defining a cyber “situation” (L) 	<ul style="list-style-type: none"> • Mapping human perceptual skills to representations of cyber situations (F) • Integration of autonomic “triage” with human decision-making for complex cyber situations (L) • Foundations for cyber data fusion (L) 	<ul style="list-style-type: none"> • Mapping human intuitive reactions to representations of cyber situations (F) • Optimization of human-cyber responses to complex cyber situations (L) • Foundations for projecting adversary trajectories through cyberspace (L)

In part, improvements in SA for cyber C2 and ISR will depend on advances in the management of “big data” since, along with all our physical space sensors, cyber sensors produce massive quantities of data. More fundamental advances are also required, such as data fusion techniques for cyber data. Unlike physical-space sensors that can be characterized and fused based on the laws of physics, cyber sensors have no known underlying relationships that allow their various outputs to be combined into single, more robust picture of reality. Likewise, no known physical laws limit adversary “trajectories” through Blue cyberspace. Development of analytics that turn low-level cyber data into meaningful entities reflective of a cyber situation has been the work of decades; this area of S&T needs significant acceleration and the injection of new ideas.

The visualization of cyber situations is another HMI that requires S&T advances. While evolution has prepared the human brain to turn millions of pixels into a visual representation in which targets and weapons are related in physical space, nothing has prepared us to turn millions of data packets into a comparable understanding of cyber threats in the mission space. Decades of experimental and heuristic approaches have resulted, at best, in visualizations of very low-level cyber data that allow some human operators to observe anomalies after extensive experience with the nominal patterns. None have resulted in an inherent understanding of the meaning of the anomalies, or an instinctive reaction that fits the cyber need. Here, advanced research in human perception and cognition is needed, along with a high-level view of what defines a “cyber situation”.

Finally, cyber C2 requires a blending of human-controlled and autonomous system controls. Ultimately, C2 and ISR for the cyber defense mission requires highly synchronized human and

machine actions that scale to full autonomic responses consistent with the cyber threats posed. These include advanced anomaly detection capabilities that trigger dynamically generated courses of action, that self-heal or self-configure as a first level of repair until the operator is inserted into the loop. In the near term, the AF should continue research into reliable detection of anomalies that can be autonomously addressed. To address this over the mid and far term requires a systematic development of automated support and close integration with optimized human-machine technologies.

6.4.3 Resilience and Agility

C2 and ISR resilience can be achieved at the mission level (wherein AF C2 and ISR is resilient to degradation in the underlying cyber support) and at the network level (wherein the cyber support to physical-space C2 and ISR is resilient to adversary attack). The advances in S&T described here enable the latter capability, as summarized in Table 6.3.

Table 6.3: Resilience and Agility

Area	Near (FY12-FY15)	Mid (FY16-20)	Far (FY21-25)
Agility and Resilience	<ul style="list-style-type: none"> • Secure Clouds (F) • Cloud-based implementations of AF C2 and ISR functions (L) • Analysis of Moving Target Defense (F) • Integrated Air, Space and Cyber Plans (L) 	<ul style="list-style-type: none"> • Identification of the Point of Compromise (L) • Secure Manual Rollback to an Uncompromised State (F) • Agile Integrated Operations Planning (L) • Sequencing Kinetic & Non-Kinetic Actions (L) 	<ul style="list-style-type: none"> • Automatic Compromise Detection (F) • Dynamic Rollback (F) • Living Plan for Agile Operations (L) • Sequencing OCO and DCO Actions (L)

Over-provisioning bandwidth provides resilience to congestion, whether self-imposed or caused by adversary action; hybrid RF-optical air-to-air links will provide high volume data capacity across the battle space. In a limited bandwidth environment, dynamic management of network resources can provide resilience to congestion. Dynamic spectrum allocation is a near-term technology that can provide more optimal bandwidth use. In longer timeframes, spatially-multiplexed multiple-in multiple-out (MIMO) capabilities can provide bandwidth augmentation and security. Far-term capability will be centered on autonomy and fully composable systems. S&T in cognitive network nodes will enable autonomous coordinated flight operation of fractional elements using short-range, low-bandwidth, jam-resistant, secure communication links. As the Air Force maps its missions to cyber dependencies, that mapping can be used to create mission-aware network services that ensure prompt delivery of critical information to support mission execution. To prevent these technologies from merely increasing the attack surface, S&T in data provenance and integrity is required.

In the near term, processing resilience is provided by cloud (or cloud-like) processing capabilities, ensuring that C2 and ISR functions can be carried out even if some subset of the processing nodes are compromised or otherwise rendered inoperable. Since the commercial

world is developing cloud computing technology, and the intelligence community is leading the development of military-grade cloud security, the AF should concentrate its near-term efforts on recasting ISR and planning processing needs into forms that can be transferred to the cloud. In the mid term, resilience research must lead to a robust capability to restore functionality lost to cyber attack. This research must include the capability to identify the moment of compromise and rollback to a safe state, as well as the out-of-band C2 and trusted functions to perform the rollback. In the long-term, the development of reliable and trustworthy autonomic cyber C2 can dynamically meet threats and reconfigure to foil them.



One way to provide resilience is through agility, another broad term encompassing many technologies. Today, moving-target defense is the focus of agility research. In the near term, many of these technologies, such as IP-hopping, will be ready for incorporation into AF networks. Careful analysis of the efficacy of moving target defenses is recommended before investing in them; some provide surprisingly little value when analyzed. Effective cyber agility must be matched to the adversary's timeline for planning and executing an operationally impactful attack; targets that move more slowly than the adversary's timeline will not have a negative effect, while movements made far more often will incur unnecessary cost to achieve the same effect. In the near term, the AF needs research into the fundamental frequency (e.g., the frequency of IP hopping) needed to make moving-target defenses effective against anticipated attack paths, while incorporating existing moving target defenses that are cost effective. In the mid and far term, continued research focused on the effectiveness of agility will result in new cost-effective agility techniques.

In the mid- and long-term, research is needed to enable agile operations planning, both for cyber defense, and for integration of cyber offense into air and space operations. An advanced planning concept is required that enables rapid plan adaption with changes in the battlespace, force status, and rules of engagement. This "living plan" will allow operators to branch off and work their sub-plans at their own pace, and then later merge them. Portions of the plan can be developed using a combination of software agents and human operators. Triggers from software agents will alert planners to changes in critical conditions that warrant a plan revision or development of an entirely new plan. Optimization algorithms and constraint schedulers provide options in near real-time that meet objectives while minimizing impact to the entire plan and combining limited resources to achieve goals as efficiently and effectively as possible. Technologies such as machine-machine workflow synchronization, applied neuroscience for human-human and human-machine collaboration, and knowledge base advisable planning and scheduling algorithms all play a pivotal role in realizing an agile, synchronized/integrated air, space, and cyber domain to achieve effects.

6.4.4 Foundations of Trust

An essential aspect of C2 and ISR in any domain is trust in the integrity of the data, whether it is the ISR upon which decisions will be made, or the C2 that results. Not only is the potential effect of an integrity failure catastrophic, but it also entails a loss of availability, since the warfighter who does not trust the information he receives will not use it. Table 6.4 consolidates the S&T focus areas for trusted foundations.

Table 6.4: Foundations of Trust

Area	Near (F12-FY15)	Mid (FY16-20)	Far (FY21-25)
Foundations of Trust	<ul style="list-style-type: none"> • Commercial HW support for platform attestation (F) • Faster, more secure cryptographic technology (F) • Dynamic keying (F) • Anti-tamper protection for software in adversary territory (L) 	<ul style="list-style-type: none"> • Trusted foundry or verified HW support for platform attestation (F) • N-version verification of information integrity (L) • Anti-tamper protection for devices in the field (L) 	<ul style="list-style-type: none"> • Contextual verification for information integrity (L)

Today, as for the foreseeable future, the foundation of preventing integrity attacks is cryptography. S&T that creates more secure cryptographic techniques and more secure implementations of those techniques (e.g., quantum cryptography) or increases the speed at which cryptographic techniques can be applied will be relevant to increased information integrity. In the near term, faster in-line encryption and disk encryption is needed. More secure hash algorithms are required. The security of cryptography depends on the security of the keys and the implementation of the algorithms. Research on secure, dynamic key distribution is needed. Group keying, that allows platforms to enter and leave groups rapidly, is especially needed for AF applications. The cryptographic checks on the provenance and integrity of information, however, will only be as good as the platform on which they are generated; that is, if the platform is not trustworthy, neither is the information it generates no matter how many hashes or certificates accompany it.

C2 and ISR information integrity specifically requires platform attestation; that is, a mechanism to attest in a provable way that the information comes from the platform it purports to, and that the platform configuration itself has integrity. In the short term, commercially supplied hardware root of trust (for example the Trusted Platform Module (TPM) and IBM SecureBlue++) can be used to anchor platform integrity attestation. Digital watermarking of ISR products can ensure data integrity from and protection of the source as information provenance is tracked throughout the enterprise. In the mid and long term, the integrity of this hardware support itself must be guaranteed, through fabrication in a trusted foundry or through the ability to analyze chip-level electronics fabricated elsewhere.

The dependence of integrity on cryptography can be reduced through new S&T. Routine refresh of static information, and comparison of multiple, independently transmitted copies of

information are two possible lines of research. The ability to identify false information automatically by considering it in the context of other information is ultimately desirable.

Finally, trust in information will require anti-tamper technology that will not allow a captured device to insert false information into the network with the imprimatur of a valid device. Technology must be developed that, like periodic re-authentication, limits the use of a device that is out of Blue hands, but unlike periodic re-authentication does not impose a burden on the warfighter in the field. Additional technology will be needed to prevent cyber agents captured by Red from being used to falsify information, especially BDA.

6.5 Conclusion

C2 and ISR forms the backbone of military planning, operational execution, and assessment. The vision outlined by the CSAF recognized C2 and ISR as one of the few areas of growth in a time of austerity. Anti-Access and Area Denial environments demand a decision advantage. In the future, leaner forces will achieve potency only when massed for effect at the right time and the right place. The permissive environments we have enjoyed during recent counter-insurgency operations have deflected attention from our cyber vulnerability and our current inability to integrate cyber, air, and space C2 and ISR. Future adversaries will take advantage of these weaknesses unless the AF addresses them forcefully.

7. Enabling Science and Technology for Cyberspace

Enabling Science and Technology is a central and cross-cutting component of the overall Air Force approach to achieving the objectives of Cyber Vision 2025. This section illuminates key findings and recommendations from other sections of this report in the context of the four technical focus areas: Foundations, Agility and Resilience, Human Social/Machine Systems, and Mission Assurance and Empowerment (see Table 7.1). This section is intended to identify and highlight key science and technology elements necessary to achieve the Air Force mission in the cyber domain.

7.1 Technology Area Overview

7.1.1 Foundations

Assessments of cyber systems in terms of modeling and measurement are critical to successful Air Force cyber operations. Issues of software and cyber system verification and validation cut across all Cyber Vision 2025 report sections. Many Air Force cyber information systems are reliant upon commercial off-the-shelf solutions. Currently, there is a tyranny of timescale; system vulnerability analysis and testing is time and labor intensive, with few ways to identify vulnerabilities before they occur. This challenge will be exacerbated in emerging fractionated systems with increasingly complex software. In order to address these issues, emphasis should be placed on automated analysis, verification, and validation of systems, as well as on developing a fundamental taxonomy of system vulnerability for information system architectures. Findings that relate to Foundations were discussed extensively in the air domain

section, as well as in the space and cyber domain sections. Enabling Science and Technology also touches on quantum analysis of systems, which was discussed in the space section.

Table 7.1: Enabling S&T for Cyberspace

Area	Near (FY12-15)	Mid (FY16-20)	Far (FY21-25)
Foundations	Measurement, Analysis, & Verification	Taxonomy of System Vulnerability	Quantum Methods for Vulnerability Assessment and Security
Agility and Resilience	Secure Virtualization for Critical Infrastructure (e.g. the AOC)	Online Vulnerability Identification, Adaptation and System Repair	Autonomous Physically Secure Cyber Systems
Human/ Social/ Machine Systems	Advanced Situational Awareness for Cyber Operators	Online Assessment of Cyber Operator Performance	Cyber Operator Performance Augmentation
Mission Assurance and Empowerment	Mission Mapping to Systems Components	Cyber Mission Verification Across Sensors/Platforms	Dynamic Cyber Mission Configuration

7.1.2 Agility and Resilience

Current cyber architectures are static, and difficult to protect given the dynamic nature of vulnerabilities and system compromises. This issue will become increasingly problematic as systems become more complex. There are few built-in safeguards that can assess and react to cyber-attacks within the timelines needed to be effective. Mission-specific adaptive methods and system architectures must be constructed so as to enable rapid response to such dynamic threats. This area includes many areas of Complex Networks and Systems theory, as well as the issues with “big data”, which were highlighted in the cyber section and the C2 and ISR section.

7.1.3 Human/Social/Machine Systems

Air Force systems have an increasing volume of information while the timeline for decision making is decreasing. This paradox is placing a significant burden on the operators of large cyber information systems. Advanced systems for cyber operator situational awareness are needed. Additionally, it is difficult to select, train and equip human operators of cyber infrastructures to be effective against a rapidly evolving threat. It is critical that the Air Force understand the optimal combination of human and automated functions in the administration of large information infrastructures. Techniques for evaluating human performance and the optimal means of augmenting human performance and enhancing human-in-the-loop, as well as human-on-the-loop, responsibilities are critical, as noted in the C2 and ISR section.

7.1.4 Mission Assurance and Empowerment

Traceability of mission performance for determining risk and enabling the commander to have accurate assessments for cyber situational awareness becomes increasingly more difficult as the operational infrastructure becomes ever more dependent upon a complex cyber infrastructure. The mission assurance and empowerment area involves assessing large mission architectures for their viability in achieving mission objectives linked to critical system components. These

needs were highlighted in all areas of *Cyber Vision 2025* but principally in the threat, cyber domain, and air domain sections of this document.

7.2 Enabling Technology Examples

7.2.1 Foundations

There are several examples of enabling technologies under the Foundations focus area beginning with methods in model checking, verification, and validation. Model checking is essentially a mathematical approach adapted to computer science for verification of computer software. These approaches have also been extended to hardware and network analysis, as well as systems security analysis. Software verification is derived from the logical state of execution of a piece of computer software. Verification methods of this sort are discussed extensively in the Air Domain section under “Reduce complexity and enable verification”.

A significant challenge when introducing software into large distributed infrastructures, such as cloud architectures or fractionated systems, is that a large dimensionality and software dependence occurs over uncertain network and hardware states. These network and hardware states can be checked just like software states but since their dimensionality and variability is so high, it is easier to represent the states as probability distributions. Such approaches are discussed in the Cyber Domain report section under “Assure Missions and Protect Critical Information in Fragile Architectures.”

Mathematical methods also have deep roots in physics-based approaches and form the basis for quantum information network, computing, and systems design. There is growing research in quantum networks and quantum computing with respect to cyber, particularly with the advent of room temperature optical semiconductors. Quantum strategies for assessment of vulnerability and security could be important for Air Force systems, since these provide the potential for enhanced security in communication, hardware and software on-chip information transfer, and within computing architectures. Such strategies hold the promise of instantaneous resistance to system compromise and threat. This is described in the Space section under “Far term: Verified Code Generation, Intent Detection, Cognitive Communications, Space Quantum Key Distribution” and is described more in the next section on agility and resilience.

7.2.2 Agility and Resilience

Several near-term enhancements to agility and resilience were discussed in the Cyber Domain section. Additionally, providing a secure virtualization capability within the AOC enhances resilience of critical AOC services, and paves the way for migration to secure cloud computing services. For the mid and long term, it is important to understand the dynamic behavior of a cyber system in the context of networks and provide insight into its properties. This area has many theoretical roots including complex networks and systems theory, multi-scale analysis, machine learning, stochastic control theory, optimization, and large data analysis.

The basic goal of a network is to guarantee transactions of information over the infrastructure. The fundamental problem of modern networks is that they do not guarantee the integrity or confidentiality of critical information transactions, but simply transfer bits from point A to point B in order to associate content with transactions of critical information across the infrastructure, systems theory can be applied to the cyber domain in many ways with analysis techniques such as deep packet inspection and network tomography. The networked system can then be treated as a black box and analyzed with little *a-priori* knowledge of its structure.

Another important area is to examine how critical information transactions happen at short timescales where individual flows of information are coded and transacted, notionally represented in Figure 7.1. From a security standpoint, encryption and steganography are part of this trade-space. Protocols for routing and security of information flows happen at intermediate timescales. An agile instantiation of these protocols would take the form of IP hopping, as described in the cyber section. At longer timescales, it is possible to look at the structure of the overall architecture for its properties of agility and resilience. Mobile ad hoc networks have a random structure that is robust to many types of disruption, particularly in the context of tactical environments. Such networks, however, pay a penalty in terms of latency. With the use of systems analysis it should be possible to design protocols to adapt and repair cyber vulnerabilities in real time as system operating conditions change.

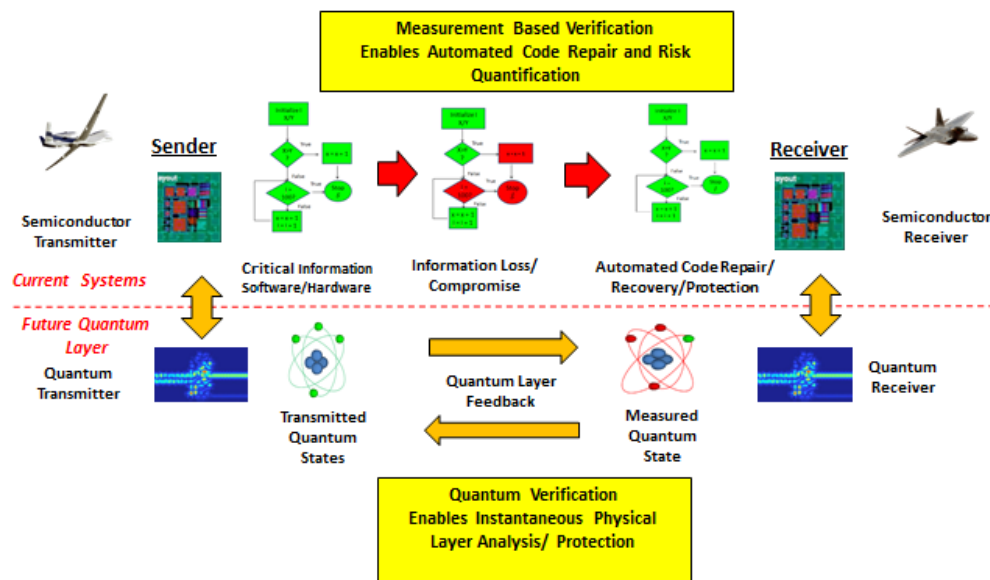


Figure 7.1: Agility and Resilience

System analysis can be applied to network, hardware, software, social networks, system control theory, and many domains in cyber using advanced machine learning techniques such as manifold learning and topological data analysis. Advanced machine learning combined with model checking and stochastic systems theory provides the basis for autonomous cyber analysis, verification, and repair of any large scale information system. This capability is

highlighted in the C2 section of the report under “Create New Massive Data Processing Capability.” This approach could also be combined with stochastic control theory for analysis of Air Force flight system components. Because this methodology is equally relevant to software and hardware, methods like artificial diversity in software and hardware architectures, and software system properties such as safety and liveliness, can also be described with this framework. This approach can be combined with automated machine learning methods for autonomous operation of cyber systems. Ultimately, this methodology extends to mission architectures and categorical analysis of correct architectures as described in the Mission Assurance section.

7.2.3 Human/Social/Machine Systems Enabling Technology

The area of Human/Social/Machine Systems brings the principles of the previous two sections to a more challenging perspective. Assessment of human behavior has traditionally been the domain of psychology and sociology. Recently, with the advent of many new means of sensing human performance using both physical sensing and computational and networking resources, techniques such as social networking analysis have become prevalent. Many of these techniques have resulted in evaluating human performance of cyber systems operators. The biggest challenge in this domain is assessing what to measure about the human, and then relating these measurements to credible sociological research for online assessment of cyber operator performance. This is described in the air domain section of *Cyber Vision 2025* under “Enable Fighting Through and Train Operators.” Stable metrics for human performance are a challenge because in many cases behavior is both context and individual dependent. The final goal is to augment human performance using autonomous system management techniques.

7.2.4 Mission Assurance and Empowerment Enabling Technology

The Air Force would like to measure our infrastructure and assess mission risk as it dynamically evolves (Figure 7.2). This point is brought out in the air and cyber sections of the report under “Science and Technology Solutions” (Air), and Trusted Foundations (Cyber). Inasmuch as this goal requires the ability to rapidly measure and assess the performance of complex systems, it depends on enabling technology efforts to gain as comprehensive a look into system performance as possible. Assessing mission risk can be accomplished at two stages. The first would be assessment of verification risk. The Air Force must measure its systems with sufficient fidelity to minimize uncertainty about actual circumstances in the infrastructure. This is a computational and resource challenge. Second, the Air Force must analyze validation risk. This asks whether the right things are being measured and assessed in order to model ‘good’ or ‘bad’ mission performance to a sufficient fidelity to compare current conditions. Finally, rather than being static, cyber domain models are dynamic and depend on the timescale of the vulnerability of interest. Constant feedback and system measurement are required to verify mission performance. Scenarios in mission performance can be posed in terms of game theoretic approaches and autonomous system management. This approach is illustrated in Figure 7.2.

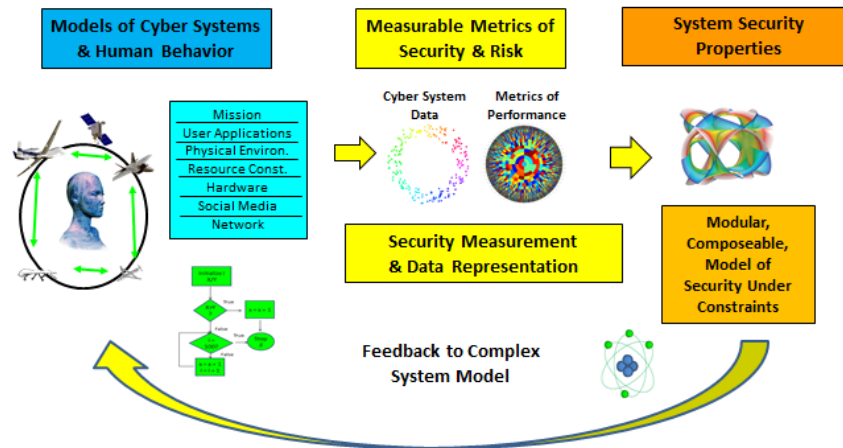


Figure 7.2: Assess Risk and Assure Mission

7.3 Air Force Research: Near, Mid, and Far Term

7.3.1 Foundations

In the near term, methods of measurement analysis and verification should be developed. Basic methods of analytic model checking are well represented in federal investments today by agencies such as the National Science Foundation (NSF) and NASA. What is not well represented, except by initial Air Force efforts, is research in measurement-based probabilistic verification methods. These methods are heavily informed by analytic and probabilistic model checking, and enable the measurement of systems that are not pre-specified where the specification is not known *a-priori*. In the mid term, taxonomy of models for vulnerability can be made as more system measurements are compiled. These strategies are relevant to methods in system identification and reverse engineering. They also lead to the ability to model check from network, software, hardware, C2, and ISR state spaces collectively, and do so dynamically rather than pre-specifying a static model. Statistical measurement and verification in quantum systems are also important in the far term.

7.3.2 Agility and Resilience

In the near term, the Air Force needs to quantify system risk and create agile management algorithms. There has been little work in verification and validation risk assessment in terms of measurement-based assessment of distributed cyber systems and integration into new physically secure variants in the quantum domain. In the mid term, it is critical to extend this concept to automated software repair and analysis, including a taxonomy of cyber vulnerabilities, and the ability to repair and dynamically assess software at the binary level. The Air Force will continue to follow work in the context of design of experiments in network risk analysis being done by institutions such as the NSF. This parallels work for automated software and repair on airborne and space platforms which the Air Force traditionally leads. Distinguishing characteristics of cyber vulnerability versus normal bugs in software is a significant challenge. Finally,

autonomous and online repair of vulnerable systems is the objective of agile and resilient systems in the far term. These systems should repair vulnerability autonomously given that there are taxonomies of vulnerability that allow algorithms (such as machine learning strategies) to discover, identify, and correct classes of system compromises. If implemented with quantum methods these methods would be highly agile and physically secure.

7.3.3 Human/Social/Machine Systems

In the near term, the Air Force will assess and measure human operators' ability to have comprehensive cyber situational awareness. An area for Air Force leadership is human performance measurement in the control loop of cyber systems. This is unlike the commercial ability to assess preference by humans in social networks, or commercial crowd sourcing large software infrastructures, areas that can be followed and leveraged. The Air Force objective is autonomous assessment of humans in cyber operations, and the ability to decide when to put humans in and out of the cyber management loop. In the mid term, the Air Force will enable real-time assessment of cyber operator performance. Real-time assessment could dovetail into the goal of the Foundations and Mission Assurance areas by providing a different measurement of complex system performance. This approach parallels technologies for pilots inside and outside the air platform control loop, which is an area that the Air Force leads. Data analysis and inference in the brain-machine interface enables interpretation of human performance in cyber scenarios. Thus, in the far term, the Air Force will enable augmented autonomous methods for cyber operators to achieve their mission objectives. Such capability could be enabled by autonomous cyber systems that repair vulnerability with minimal user intervention, and real-time assessments of cyber operators with feedback of cyber operator performance.

7.3.4 Mission Assurance and Empowerment

In the near term, the Air Force should be able to map a mission to specific system and human performance functions. There is very little work in federal agencies, commercial industry, or academia in terms of mapping mission functions to network and system infrastructure components. This capability is critical for Air Force cyber operations and vulnerability assessments. Combining reconnaissance information and automatic target recognition with mission mapping in the cyber domain is another critical capability that does not exist in the DoD. The Air Force needs cyber mission situational awareness across its ISR and air platforms. The Air Force has significant technical strength in this area because of its traditional roles in C2 and ISR missions. Automated mission planning, analysis, and adaptation based on incoming data and situational awareness is also critical for agility in the cyber mission domain. This research is different than online network/cloud policy management in the commercial domain. Finally, the Air Force needs to dynamically and autonomously reconfigure its operations as conditions change. Such reconfiguration would be based on dynamic autonomous assessment and management of infrastructure, and human operators that have been identified as mission critical.

8. Mission Support

Cyber Vision 2025 emphasizes revolutionary cyber technologies and approaches that address the challenging complexity of future Air Force cyber missions. The Mission Support section of this document examines four areas: the aspects of cyber acquisition that must adapt to enable advanced technologies in a flexible and responsive manner; rigorous test and evaluation standards and policy to ensure the full-spectrum effectiveness and security of the variety of Air Force weapon systems; education programs that provide sufficient quality and quantity of talent to meet civilian and military accession and recruiting requirements; training programs designed to stay one step ahead of growing adversary capabilities by obtaining exquisite insight, both for cyber-specific workforce professionals, as well as acquisition and test personnel working across all domains; and strategic career development of cyber professionals to ensure the best and brightest are grown and properly utilized in the evolving cyber battlespace of 2025. The following sections examine the findings in each of these areas, and offer recommendations to address the issues discussed.

8.1 Cyber Acquisition

Cyber acquisition is generally viewed as not responsive to warfighter needs, delivering systems that are late-to-need or obsolete before they make it to fielding. The 2009 Defense Science Board Report on *DoD Policies and Procedures for the Acquisition of Information Technology* well documented this challenge. Cyber acquisition consists of two categories: the acquisition of cyber systems, to which the above critique applies, and the acquisition of cyber-physical systems, which is discussed in greater detail in following sections. In many cases the critiques levied on the acquisition of cyber systems are valid, and are largely artifacts of applying processes from major weapon system acquisition programs to the world of cyber warfare capabilities, command and control systems, and other information system and information technology efforts. The following sections discuss these separate categories, and offer some recommendations to address their unique challenges.

8.1.1 Acquisition of Cyber Systems

For the purpose of this section, “cyber systems” refers to “information systems” as defined by Joint Publication 3-13 and, more specifically, those tools and systems for Offensive Cyberspace Operations (OCO), Defensive Cyberspace Operations (DCO) and DoD Global Information Grid Operations (DGO), in addition to command and control systems and networks (AOC weapon systems, satellite ground segment systems, RPA C2 systems, etc). Essentially, “cyber systems” refers to those systems comprised primarily of software and associated computing hardware and networks, and generally do not interface with or directly influence the real world (as opposed to cyber-physical systems, as defined in the next section).

One subset of cyber system acquisition is referred to as “cyber warfare capability acquisition” in the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) Section 933 Report to Congress, which includes capabilities supporting OCO, DCO, and DGO. Through the Section 933 Report, USD(AT&L) will assume a stronger role in acquiring cyber

warfare capabilities, and has divided this area into two categories -- Rapid Cyber Acquisition and Deliberate Cyber Acquisition. The *rapid* process aims to satisfy requirements within a timeframe of days to months to address operationally urgent needs, while the *deliberate* process aligns with emerging IT acquisition streamlining efforts to develop capabilities within 18 months or less. The Air Force acquisition organization responsible for these categories of systems – the former Electronic Systems Center (ESC) now within Air Force Materiel Command/Air Force Life Cycle Management Center (AFMC/AFLCMC) – has restructured its organization and processes to enable more responsive cyber acquisition, and their efforts align with those of USD(AT&L). Currently DoDI 5000.02, the Department instruction governing all acquisition programs, is under revision and may include further changes that enable more responsive cyber system acquisition. In addition, the Air Force acquisition community should continue to monitor government and industry for best practices that could be adapted or adopted to enhance/improve cyber system acquisition.

The recent policy and process changes referenced in the Section 933 report have not had time to influence current acquisition programs, but promise to do so in a positive way. Incorporating flexible funding options, to include a “working capital fund” structure, will help enable responsive cyber acquisition to warfighter needs. The Air Force realignment and reorganization to enable more responsive cyber acquisition also have not had an opportunity to prove fruitful.

The segment of cyber systems not covered by the Section 933 report includes various command and control systems. Best practices discovered by ESC’s efforts related to Section 933, as well as updates to DoDI 5000.02, need to be incorporated into these C2 weapon system programs as well. Specific recommendations concerning these systems can be found in the air, space, and C2 and ISR mission area sections of the *Cyber Vision 2025* document, in addition to the recommendations at the end of this section.

8.1.2 Acquisition of Cyber-physical Systems²

While information systems and computer networks receive much of the attention when it comes to cyber, 98% of all processors are found in embedded systems, not PCs or computer servers. These embedded processors make up the foundational capability of nearly every weapon system in the Air Force inventory, to include associated base support and maintenance infrastructure, and these systems should be viewed as “cyber-physical systems².” While the term *cyber-physical* has been around since 2006, the average individual does not immediately think of aircraft, space vehicles, launch platforms, missiles, and the myriad other weapons systems as not merely cyber-*dependent* platforms, but essentially cyber systems themselves.

² For the purpose of this section, “cyber-physical systems” refer to those systems with a tight integration between the physical, computational and networking elements, and which directly interface with and influence the real world. This term includes and expands upon “embedded systems,” and was coined by Helen Gill of the National Science Foundation in 2006. Due to the complex nature of modern weapon systems, this includes all modern aircraft, space systems, munitions, industrial control systems and various other systems that are not strictly “information systems.” Neither Joint nor Air Force doctrine currently defines this class of systems.

This shift in mindset is far from complete in the Air Force, but making this change is essential to the mission assurance of Air Force weapon systems and platforms. The Air Force must begin viewing its aircraft, space systems, launch platforms, munitions, industrial control systems and other operational and support systems as vulnerable not just to opposing threats within their operational domain, but also potentially vulnerable to many different cyber attack vectors.



The concept of a “standalone network” or “air-gapped system” has never truly existed, as evidenced by the Stuxnet attack against a supposedly “closed” Iranian nuclear processing system.

One problem is that cyber-physical systems often contain subsystems or support equipment that is declared “platform IT;” this equipment is exempted or waived from sufficient cyber system-level vulnerability or security testing, as it does not connect directly to an Air Force network or the GIG. The Air Force must immediately stop granting waivers for this class of systems, as it could inadvertently open the system to a cyber attack vector that compromises the ability to conduct its mission. Mission assurance is paramount for all current and future Air Force weapon systems. A proposed approach to achieve mission assurance is conducting Cyber Assessment and Vulnerability Evaluations, discussed later in this section.

8.1.3 Cyber and Cyber-physical System Requirements

Various aspects of system security from a cyber perspective are currently overlooked in many acquisition programs. The term “cyber security” does not quite encompass the total requirement for “system security from a cyber perspective” -- that is, examining the total weapon system for potential and realized vulnerabilities that could be exploited through cyber methods, rather than the subsets of information security, information assurance, network security, and others. Recent studies have demonstrated the vulnerability of weapon systems to cyber attack vectors that could potentially cause complete mission failure (see details in the classified annex). The Air Force must ensure these vulnerabilities are reduced or eliminated through sound system engineering, which currently does not include the appropriate level of attention for cyber-physical systems.

The Air Force must create cyber system security requirements that encompass all potential cyber attack vectors, and ensure that these requirements are placed on all Air Force cyber and cyber-physical programs. While some systems have been designed with certain levels of cyber system security in place, and are indeed resistant and/or resilient to various cyber attacks, the unfortunate majority of systems have not. The Air Force must enforce these cyber system security requirements across the breadth of Air Force programs. As this issue transcends Service-specific needs, the Air Force should lead an effort with USCYBERCOM, the other Services, and Department of Defense and Interagency partners to implement these future Air Force standards across the range of national security systems. This could result in the creation

and formulation of a “cyber system security” Key Performance Parameter (KPP) at a later date, but the Air Force must endeavor to ensure these requirements do not devolve into paper-based and checklist-focused efforts, but rather tangible and testable requirements.

8.1.4 Cyber Assessment and Vulnerability Evaluations³

As requirements mature and become standardized across Air Force weapon systems, the ability to appropriately test and verify these requirements becomes paramount. As discussed in earlier sections and the following T&E section, full-spectrum vulnerability assessments - fully integrated into the acquisition process - are required to guarantee mission assurance in the future cyber battlespace of 2025.

The Air Force and other agencies have some red team and blue team efforts to assess various weapon systems. Red teams traditionally take the perspective of an informed adversary, and seek to attack using similar methods as the adversary, although they typically have limited time, resources, and legal authorities. Blue teams often assume the role of “defender” against the red teams, with the goal of preventing the red team from accomplishing their mission. While these are good first steps, they are not sufficient to defend against the range of cyber threats facing the Air Force weapon system portfolio. There is a need to slowly increment the ability to show realism in DoD exercises as opposed to the current state of red team dominance.

The Air Force must immediately begin developing and institutionalizing Cyber Assessment and Vulnerability Evaluations (CAVEs) throughout the acquisition life-cycle. Essentially, a CAVE includes elements of red and blue team assessments, but is more thorough. CAVEs would require a new level of elite future cyber warriors, discussed later in the Workforce section. The *independent* evaluation team would include experienced and well-educated individuals from outside the program office, would be granted “insider” access to program information (wiring/network diagrams, architecture layouts, source code, etc.), and would receive unfettered access to program engineers (including contractor personnel). It is imperative that these elite team members maintain currency in the constant change in the knowledge base in cyber operations. The knowledge base is perishable and becomes obsolete in a short period of time. The team would have the mandate to conduct unbounded and full-spectrum assessments using any potential cyber attack vector. This exceeds the current charter for red teams, which often must make assumptions about adversary capabilities, which limits their discovery and exploitation of all *potential* attack vectors. They would assess the system at multiple points in the system life-cycle, from the design phase through early design, prototyping, DT&E, OT&E, fielding and into sustainment. As needed, they could assist the program office or sustainment organization with mitigation efforts. When cyber threats affect operational platforms, they would provide the critical experts to identify, diagnose, and fight through cyber attacks.

³ More detail on the recommended methodology is found in the recent work of Dr. Jonathan Butts and others from the Air Force Institute of Technology, a framework which can be applied to all weapon systems.

8.1.5 Cyber Acquisition Recommendations

1. **Expand, enhance, and institutionalize full-spectrum Cyber Assessment and Vulnerability Evaluations across the Air Force portfolio of cyber and cyber-physical systems throughout the life cycle.** The backbone of mission assurance must be thorough, unbounded, and full-spectrum cyber assessments, conducted by appropriate teams of operators, engineers, scientists, contractors, and other system experts. Today's red team or blue team constructs are insufficient to fully secure systems from a cyber perspective (OPR: SAF/AQ, OCR: AFMC, AFSPC, AF/TE)
2. **Create, standardize, and implement cyber system security as an integral part of the requirements and systems engineering process.** Ensuring system-level requirements for security from a cyber perspective are created and mandated across Air Force weapon systems is the foundation for mission assurance in a contested cyber environment. (OPR: SAF/AQ, OCR: AFMC, AFSPC)
3. **Overhaul efforts to streamline cyber acquisition policy and processes, and periodically reassess to determine effectiveness; implement best practices within acquisition of the wide range of information systems.** The Air Force is making progress in this area in concert with USD(AT&L), and needs to ensure follow-through and assessment of progress, and application to other areas outside the AFMC/AFLCMC portfolio. (OPR: SAF/AQ, OCR: AFMC/AFLCMC, AFSPC)
4. **Develop flexible funding authorities to become fully responsive to warfighter needs.** The Section 933 efforts may prove fruitful in this area, but the Air Force must advocate for and ensure this flexible funding endures to enable truly responsive cyber acquisition. (OPR: AF/A8, OCR: SAF/FM, SAF/AQ)

8.2 Test and Evaluation

For both cyber and cyber-physical systems, the need for OT&E is often considered a one-time event prior to system fielding, which is too late to make any substantive changes when problems are identified. Greater efficiencies are possible when the requirements, acquisition and T&E communities begin close collaboration before program initiation and continue throughout the entire program lifecycle. Key stakeholders from multiple disciplines must integrate their efforts to produce efficient schedules, eliminate “stovepipes”, share information in open T&E databases, identify problems early, engage contractors to fix deficiencies sooner, and ensure systems are ready to enter dedicated operational testing with a high probability of success.



In addition, T&E efforts generally focus on one-dimensional functionality (i.e. “does this input provide the desired output?”) without regard for security considerations (i.e. “are there inputs that provide undesired outputs?” or “are there vulnerabilities that would allow the system to fail

its mission?”). While the Certification and Accreditation (C&A) process is intended to address *some* of these issues, it has proven itself insufficient for today’s increasingly complex cyber and cyber-physical systems--it is largely a checklist-focused effort that rarely involves sufficient hands-on testing or assessment.

Vulnerability assessments are not mandated by any institutionalized process. Program managers decide whether or not to schedule and fund an assessment. According to AF/TE, of 43 assessments conducted since 2009 by the Air Force’s “blue team” cyber unit, none were performed during Developmental Testing. All assessments were accomplished either after the system was already fielded (65%) or during Operational Testing (35%). It is also significant to note that only 43 of 451 programs have conducted an assessment since 2009. The critical value added by these assessments comes much too late as security must be designed into a system -- like stealth capabilities, it cannot be added nor tested after the fact.

8.2.1 Certification and Accreditation Shortfalls

The current Certification & Accreditation process model must evolve to integrate full-spectrum cyber-focused vulnerability assessments for cyber and cyber-physical systems, as discussed earlier. These assessments must begin at the requirements definition and early design phase and be accomplished continuously throughout the acquisition life-cycle. As discussed in the Acquisition section, better requirements are needed for total system security from a cyber perspective, as well as increased numbers of better educated, trained, developed and experienced cyber professionals within the T&E community; these individuals are needed to help during requirements definition and in the design and execution of both developmental and operational tests.

In order to achieve the goal of fielding systems that both operate as designed and are *secure* in their design from a cyber perspective, the Air Force must ensure program managers are graded not just on cost/schedule/performance metrics, but also on the result of the full-spectrum cyber vulnerability assessments conducted against their systems. Current C&A processes are costly without adding sufficient value to programs, and as such they are seen as a “necessary evil” rather than embraced as an opportunity to reduce vulnerabilities and assure mission success.

8.2.2 Test and Evaluation Infrastructure

Cyber test and training ranges have been developed and utilized without central requirements, funding, or authorities. The Air Force and Department of Defense have many cyber test ranges, but are unable to declare whether that test infrastructure is adequate to meet current and future testing needs for cyber and cyber-physical systems.

The recent Section 933 report to Congress outlined the Department of Defense’s goal of improving oversight and minimizing duplication of cyber test infrastructure, which is a good first step. The Air Force must develop a way to manage service-specific test infrastructure using a centralized inventory and capabilities database. Appropriate gap analysis is needed to identify

requirements and capabilities not currently available, and for better advocacy with the Section 933 organization that will handle cyber test infrastructure at the Department level.

8.2.3 Test and Evaluation Recommendations

1. **Cyber Test & Evaluation must begin at the requirements development and design phase, and be accomplished continuously throughout the acquisition life-cycle.** Testers must be integrated as early as possible, from requirements definition, initial design, Tactics, Techniques and Procedures (TTPs) development, and all the way through fielding and sustainment.
(OPR: AF/TE, OCR: SAF/AQ)
2. **The Air Force must overhaul the current Certification & Accreditation and checklist-focused model to full-spectrum and unbounded vulnerability assessments of cyber and cyber-physical systems.** The days of paper-based C&A with little to no hands-on system assessment must end. Testing programs must include Cyber Assessment and Vulnerability Evaluations prior to, and during, developmental test and evaluation, in addition to system functional testing, and throughout the life-cycle
(OPR: AF/TE, OCR: SAF/AQ, AFMC, AFSPC)
3. **Develop a centralized inventory and capability database for cyber test infrastructure, and conduct gap analysis to identify cyber range requirements and capabilities.** Under the Section 933 report, USD(AT&L) will assume a role in managing DoD cyber test infrastructure. The Air Force must embrace this new process, and lead the effort to ensure Air Force-specific requirements are identified, funded, and developed.
(OPR: AF/TE, OCR: AFSPC, AFMC)

8.3 Education and Training

The Air Force is entirely dependent on U.S. educational institutions to provide the cyber talent required for its workforce. While direct influence is limited, there are areas where the Air Force can make an impact, specifically within the U.S. Air Force Academy (USAFA) and ROTC programs. Additionally, the Air Force possesses organic graduate cyber education capabilities within the Air Force Institute of Technology. As adversary capabilities grow, it will become increasingly necessary for the Air Force to recruit and retain the brightest scientists, engineers, and cyber operators with the right education in cyber fundamentals, and then train those individuals in the art of cyber warfare. The field of practice will continue to be Air Force and Joint exercises, to include Cyber Flag, Red Flag and other opportunities to deploy and operate weapons systems in a contested cyber environment.

8.3.1 Accessing Cyber Talent into the Air Force

The U.S. university system is not producing the required quantity and quality of students educated in cyber specialties to compete with growing adversary capabilities. The number of undergraduate degrees granted in Science, Technology, Engineering and Mathematics (STEM), and specifically cyber specialties (Computer Engineering, Electrical Engineering, Computer Science and Mathematics), has declined over the past decade. Further reducing the number of

available qualified graduates, many of the international students at U.S. institutions who once stayed and worked in the U.S. after graduation are now returning to employment in their home countries. To make matters worse, several government agencies and industry partners note that graduates with cyber-specific degrees lack knowledge of secure coding and trusted hardware architectures, requiring additional on-the-job training to fill these gaps.

The Air Force must advocate for and influence development of curricula that includes secure software coding, secure and trusted hardware architectures, and other areas of technical interest. By refocusing current Air Force STEM outreach funding mechanisms more towards cyber-specific areas of interest (like the Cyber Patriot program), it can influence the number of college graduates pursuing these degrees. The Air Force should partner with industry in pursuing these shared goals.

USAFA is an institution where the Air Force has direct influence over accession goals. USAFA should expand the current cyber warfare curriculum to include aspects of secure coding, trusted hardware and cyber-physical systems; continue to exploit the success found through partnering with industry via the Center of Innovation (CoI); and encourage, influence or direct incoming students to pursue cyber-specific degrees. USAFA has the potential to emerge as the premier U.S. undergraduate institution for cyber education.

The Reserve Officer Training Corps (ROTC) and Officer Training School (OTS) programs are the other institutions where the Air Force has direct control over the quality and quantity of incoming accessions. Unfortunately, from available data from 2009-2012, over 65% of non-STEM-degreed cyber operators came from the ROTC program. The Air Force must focus its limited ROTC scholarship funding to recruit cadets that will pursue degrees that are of importance to the Air Force and for which the demand will not be met without such scholarships. Over time, this will increase officer accessions in STEM and cyber specialties that have posed significant recruiting problems in the past. The Air Force cannot afford to grant scholarships to cadets to earn degrees in fields with accession quotas that can easily be met from non-scholarship cadets. Similarly, targeted recruiting quotas can be used to tailor the academic backgrounds of OTS accessions to be more responsive to the needs of the Air Force. By becoming more deliberate in ROTC and OTS accession requirements, the Air Force can ensure more qualified candidates enter the career field. While some liberal arts degrees are beneficial to the cyber career field, only those who have demonstrated aptitude and technical potential should be admitted. To help enable this concept, the Air Force is collaborating with the Navy to develop an appropriate “aptitude test” for cyber, similar to the Defense Language Aptitude Battery (DLAB) for assessing ability to learn a foreign language.

8.3.2 Education and Training within the Air Force

While there are several current cyber education and training programs in the Air Force, they must continue to evolve in depth, breadth, and throughput to compete with growing adversary capabilities, detailed further in the classified annex. The Air Force should lead the development

of a cyber-physical warfare graduate degree, analogous to the current AFIT cyber warfare degree. As the acknowledgement and understanding of cyber-physical systems and the various vulnerabilities and opportunities in this area grow, so must the ability to develop individuals with the required education in the “art” of both cyber and cyber-physical warfare. To close the gap between undergraduate output and mission requirements, the Air Force should expand the number of accessions who obtain advanced cyber education at AFIT directly following graduation, with a focus on both the science and the art of cyber and cyber-physical warfare.

The Air Force must include civilians in this process, and break down the current barriers to civilian attendance in Air Force education and training programs. This includes, but is not limited to, ensuring centralized funding is available to educate and train civilians alongside their military counterparts at AFIT and elsewhere. The continuity provided by a properly educated, trained, and experienced civilian cyber workforce is essential to success.

In addition to the focus on members of the “cyber professional” career fields, developers, acquirers, testers and others across the Air Force mission spectrum need not just cognizance of the various cyber and cyber-physical threats facing their platforms, but also advanced education and training on how to ensure security from a cyber perspective is included in their systems engineering processes. The Air Force must ensure these non-cyber personnel receive advanced training in cyber and cyber-physical warfare, so they may help engineer mission assurance into their respective programs.

8.3.3 Education and Training Recommendations

1. **Increase support of high school and university cyber recruitment efforts, to include intern programs, cyber competitions, and other outreach efforts.** The Air Force must leverage current STEM outreach efforts (i.e. Cyber Patriot, etc) and increase focus on activities and programs specifically related to cyber.
(OPR: AF/A1, AFSPC; OCR: SAF/AQ, SAF/CIO A6)
2. **Project future cyber workforce requirements for cyber-specific degrees (EE, CompE, CS, Math) and align with USAFA curriculum and degree production, targeted ROTC scholarships, and focused OTS recruitment.** Aligned with the Workforce recommendation regarding workforce development, the Air Force must better project the need for cyber educated accessions as missions grow across the Air Force which require technically-educated cyber professionals.
(OPR: AF/A1, AETC; OCR: AFSPC, SAF/CIO A6)
3. **Advocate and influence U.S. universities (including USAFA) to expand depth-of-coverage in secure software coding, secure & trusted architectures, and other technical areas of interest related to cyber and cyber-physical systems, while also expanding AFIT programs in these areas.** According to both government and industry partners, undergraduate and graduate education in these areas is lacking, which results in lost time and efficiency as these skills are often learned on-the-job. Future cyber professionals will need to be experts in these areas as applied to both cyber and cyber-physical systems.

(OPR: AFIT, OCR: USAFA, AFSPC)

4. **Develop and require cyber ops training at the technical level for non “cyber professional” personnel.** Education and training are paramount for the cyber workforce, but the Air Force must also ensure those individuals involved with acquiring cyber-physical systems are trained in some aspects of cyber warfare. While the workforce vision of 2025 will include cyber operations SMEs in various program offices, these individuals are only part of the solution -- cyber and cyber-physical warfare cognizance is needed across the acquisition workforce.

(OPR: SAF/CIO A6, OCR: AETC, SAF/AQ, AFMC)

5. **Provide funding and institute workforce roadmap that allows civilians to participate in the range of DoD-provided education and training opportunities alongside their military counterparts.** As a part of the Total Force, civilians supply the expertise, experience, and continuity required to respond to future cyber threats across the Air Force enterprise. The Air Force must ensure its civilian workforce is given the same deliberate development as their military counterparts.

(OPR: SAF/CIO A6, OCR: AFSPC, AETC)

8.4 Cyber Workforce Development

The demand for skilled cyber professionals -- developers, analysts, acquirers, testers and operators -- will continue increase in response to growing adversary capabilities and the need for cyber subject matter experts throughout the Air Force⁴. The foundation of progress in this area is a sound and comprehensive workforce development roadmap that identifies required future skills sets mapped to specific positions. This roadmap must include the Total Force -- officers, enlisted, civilians, reservists and National Guard members. Due to the complex and dynamic nature of the cyber environment, the current roadmap (August 2010) is already outdated and inconsistent with current operating policies.

8.4.1 Cyber Warrior of the Future

The workforce roadmap must examine and define the “cyber warrior of the future” -- in order to identify the required knowledge, skills and experience, the Air Force must first define what this person will be expected to do. Cyber operators currently generally fall into OCO, DCO, DGO or CNE roles; future cyber operators will require the ability to seamlessly flow between these roles (and others) as the battlefield evolves and missions dictate. This will lead to changes in current organizational structures, as future mission sets evolve and stovepiped organizational structures begin to constrain operations.

⁴ The Air Force has made great strides since 2009: the standup of 24th Air Force and the 17D and 1B4 career fields, revamp of Undergraduate Cyber Training, development of Cyber 200 and 300 professional development courses, first graduates of the Cyber Weapons Instructor Course, stand up of a Civilian Cyberspace Fundamentals Course, and the publication of a Cyberspace Civilian Training Guide. While these workforce advances were the necessary first steps, to maintain and improve the Air Force’s cyber advantage, it must continue to evolve.

The future cyber professional must be educated in cyber foundations, trained in the art of cyber and cyber-physical warfare, and able to seamlessly flow from the offensive to defensive role as the mission dictates. There will remain a need for dedicated defensive cyber operators in the future, focused on securing and protecting cyberspace infrastructure. In practice this may cause challenges with today's authorities, so the Air Force must work with the Department of Defense and Interagency partners to progress from Cold War-era authorities to cyber policy that better aligns mission capabilities to enable mission success.

As the cyber operator career path evolves and matures, some will rise to become Air Force Cyber Elite (ACE) operators, those able to seamlessly flow between offensive and defensive roles, and excel at both. These elite operators will also be needed as testers, red and blue team members, and CAVE team leaders. In addition, more cyber operators will be required as subject matter experts throughout air and space operations centers, intelligence organizations, and both cyber and cyber-physical program offices. Notably, the tools needed by these advanced operators will fuel innovation. The Air Force must ensure current and future accession requirements, in both quantity and quality, are aligned with this comprehensive workforce development roadmap.

8.4.2 Cyber Workforce Development

The current classification guide for officer cyber operators does not ensure the most qualified candidates fill these critical positions. Approximately 50% of the career field does not have STEM degrees, and of those that do, only half of those degrees are cyber-focused. Those with cyber-specific degrees have demonstrated the value of having these degrees - of Undergraduate Cyber Training (UCT) graduates since 2010 who were selected for advanced cyber operations training, 75% held STEM degrees and, of those STEM degrees, 75% were either Computer Engineering or Computer Science. While some individuals without STEM or cyber-specific degrees have shown an aptitude for success in this area, it is clear that cyber-focused STEM degree help ensure both an aptitude and an interest in the cyber mission area. The Air Force must change the current classification guide to ensure a minimum of 50% of accessions have a cyber-specific degree (Computer Engineering, Computer Science, Electrical Engineering, or Mathematics). Of the remaining 50%, the minimum standard should require individuals to have earned a STEM degree, with limited exceptions only for those who have demonstrated potential through cyber aptitude testing.

While military cyber operators conduct the majority of cyber operations today, this might not be so in 2025. To ensure continuity, depth and breadth of knowledge and experience, the Air Force must invest in building and developing the civilian cyber workforce. In 2011, the Air Force employed 1,334 civilians in the Computer Science and Computer Engineering occupational specialties -- a mere 15% of the total DoD inventory. While the numbers for Electronics Engineers are higher - 5,055 total Air Force civilians, a 30% share of the DoD inventory - many of these individuals are employed in non-cyber positions at laboratories and program offices.

8.4.3 Cyber Workforce Recommendations

1. **Building upon the success of red teams and hunter teams, further develop a cadre of Air Force Cyber Elite (ACE) professionals.** The cyber warrior of the future will be integral to different teams from acquisition to operations. The Air Force will rely on a very high performance cadre of “first responders” to ensure it can fight-through degraded cyber environments and assure mission success. Developing this high performance cyber force should leverage Air Force pilot training heritage from Red Flag and Fighter Weapons School within the new Cyber Flag and Cyber Weapons School as well as novel mechanisms such as virtual cyber training or “just in time” training. This will help ensure an agile cyber force adaptable to unexpected futures. (OPR: SAF/CIO A6; OCR: AFSPC, AFMC)
2. **Create an updated comprehensive workforce development roadmap to identify future skill sets and Total Force mix to preserve U.S. cyber competitive advantage.** This roadmap must outline the career path and educational requirements for the “cyber warrior of the future,” and must include the projected future operational concepts for these warriors, as well as the projected involvement of cyber SMEs across the Air Force enterprise. (OPR: SAF/CIO A6; OCR: AFSPC)
3. **Mandate a minimum requirement of 50% cyber-specific foundational degrees (EE, CompE, CS, Math) for the 17D cyber operations career field.** The future cyber operating environment will require individuals with a strong educational foundation in cyber science and engineering. (OPR: SAF/CIO A6; OCR: AF/A1, AFSPC)
4. **Eliminate the “catch all” statements that allow individuals to become cyber operators without meeting minimum educational requirements, unless they have demonstrated strong aptitude for cyber missions.** As the cyber mission set grows in complexity, the career field cannot accept individuals without a prerequisite technical foundation. However, some individuals have proven cyber aptitude without a technical degree, but these are the exception. The Air Force needs an aptitude test to assess and admit only those non-cyber educated individuals who demonstrate both interest and aptitude. (OPR: SAF/CIO A6; OCR: AFRL, AFSPC)

8.5 Conclusions

S&T advances and subsequent adoptions can lead to significant cyber capabilities to the Air Force, but only if those systems are secure from a cyber perspective through proper test and evaluation, and there are sufficient numbers of trained and educated cyber professionals who have been deliberately developed and managed. The Air Force must invest heavily in its future cyber professional workforce, both monetarily where needed, but also in the time and effort required to follow an intentional and threat-responsive workforce development roadmap. In 2025, the cyber workforce must exist in sufficient numbers and have the expertise required to achieve mission assurance and empowerment across the Air Force mission portfolio.

9. Conclusion, Summary Findings and Recommendations

Cyber Vision 2025 is an S&T vision and blueprint to help the *Air Force* achieve the “assured cyber advantage” across core Air Force missions. *Cyber Vision 2025* recognizes that all of our missions (air, space, C2, ISR) depend on cyberspace and also that many warfighting missions systems are composed of significant portions of information technology. Furthermore, the cyberspace domain is contested and/or denied. Our current environment is also characterized by constrained resources (e.g., financial, human, time) given federal deficits, limited production of U.S. computer graduates, and highly rapid attacks and threat evolution. Finally, cyberspace missions can have digital, kinetic, and human effects.

“Cyber has become a major concern as we face large numbers of attacks from non-state actors and large nations alike, and the prospect of a catastrophic disruption of critical infrastructure that would cripple our nation. The potential to paralyze this nation from a cyber attack is very real.”

Honorable Leon Panetta, Secretary of Defense
October 2011



Summary key findings of Cyber Vision 2025 include:

- Our missions are at risk in part because of the rapid increase in interdependency among systems, which drives both cost and risk but also because the risks from malicious insiders, supply chain threat, and Advanced Persistent Threat (APT)
- Cyber S&T can provide assurance, resilience, affordability, empowerment
- We need to integrate across authorities and domains
- We need to shape doctrine, policy, people, processes (RDT&E)
- Partnership and leverage are essential

An enterprise wide effort is essential to realize important benefits, therefore, as detailed in the sections above, the Air Force must:

- Assure and Empower the Mission (OPR: MAJCOMs) by:
 - Assuring national security missions to security standards exceeding business systems
 - Make more effective use of Title Authorities (e.g., 10/50/32)
 - Learn how to achieve integration and synchronization of multi-domain effects
 - Increase the cost of adversary OCO
- Improve Cyber Education, accessions, and advanced teams such as the concept of an Air Force Cyberspace Elite (ACE) (OPRs: AETC, AFSPC, A1, A6, A3)
- Advance Processes and Operations (OPRs: AFPSC, AQ, TE, MAJCOMS, A3):
 - Require/design in security; secure the full life cycle
 - Rapid, open, iterative acquisition; engage user/test early
 - Integrate cyber across all the CFMPs
 - Advance partnerships, align funding

- Advance cross-domain orchestration and synchronization of effort and effects
- Enhance Systems and Capabilities (OPRs: AFSPC, AQ, AFMC)
 - Reduce complexity and verify designed systems
 - Advance hardened, trusted, self-healing networks and information
 - Create agile, resilient, disaggregated mission architectures
 - Develop real-time cyber situational awareness/prediction, managed information objects, and cyber FME
- Partner with relevant federal government entities to leverage investments and focus Air Force S&T investments in lead, follow, or watch roles (OPR: AFRL) on efforts that will:
 - Assure and empower missions
 - Enhance agility and resilience
 - Optimize human/machine systems
 - Establish foundations of trust

Air Force leaders at all levels should make cyberspace assurance and empowerment a priority by taking concrete actions in their own units. This includes practicing sound cyber hygiene such as by always encrypting data at rest and in motion and utilizing trusted boot processes which are already available from AFRL when government computing infrastructure is not available. When requiring or designing infrastructure or systems, leaders should simplify as much as possible but retain sufficient diversity and redundancy to assure operations. They should employ compartmentalization and least privilege, balancing this with the need to share. Leaders should map their missions to identify and mitigate dependencies, identify mission critical assets (so called “crown jewels”) and disproportionately protect those. They should demand increased cyberspace situational awareness, keeping in mind supply chain, malicious insider and APT threats and continually adapting to their evolution. Finally, they should invest in themselves and their staff to deepen their understanding and leverage of cyberspace.



Realizing the full promise of *Cyber Vision 2025* will require concerted and sustained Air Force leadership and external partnership to ensure the necessary cultural change and organizational

evolution to achieve the assured cyber advantage. In addition, since no plan survives contact with the future, *Cyber Vision 2025* should be revisited at least every 10 years to update the Air Force cyberspace S&T blue print.

In conclusion, not only is cyberspace a national critical infrastructure and economic engine to be defended, it will be a center of gravity in future major military conflict. *Cyber Vision 2025* enables mission assurance and empowerment in peacetime, during humanitarian and disaster relief, or in military conflict. Working as a team, in full partnership with other services, agencies, national laboratories, FFRDCs, industry, academia, and international partners, the Air Force must advance cyberspace across air, space, cyber, C2 and ISR and mission support to ensure its future ability to fly, flight, and win in air, space, and cyberspace.

10. References

- Air Force Doctrine Document (AFDD) 2-5, *Information Operations*, 11 January 2005, 5–25; Field Manual 3-13, *Information Operations: Doctrine, Tactics, Techniques, and Procedures*, 28 November 2003,
- Air Force Doctrine Document (AFDD) 3-12, "Cyberspace Operations" July 2010.
<http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-12.pdf>
- Air Force Research Laboratory *Cyber S&T Strategy*. 2012. Draft.
- Air Force Scientific Advisory Board. *Implications of Cyber Warfare, Vol. 1: Executive Summary and Annotated Brief*. SAB-TR-07-02. Washington, DC. Aug 2007.
- Air Force Scientific Advisory Board. *Defending and Operating in Contested Cyber Domain*. SAB-TR-08-01. August 2008.
- Air Force Scientific Advisory Board. *Cyberspace Situational Awareness*. forthcoming.
- Air Force Tactics, Techniques, and Procedures, 3-1.MQ-9, 15 September 2010, "Tactical Employment MQ-9"
- Air Force Tactics, Techniques, and Procedures*, 3-3.F-35, 18 November 2010, "Combat Aircraft Fundamentals F-35"
- AFOSI Counterintelligence Assessment, 10 August 2009, "F-35 Joint Strike Fighter"
- Carroll, J. and Montgomery, K. 1 December 2008, "Global Positioning System Timing Criticality Assessment – Preliminary Performance Results"
- Charney, Scott. "Establishing End to End Trust." The Microsoft Corporation. 2008.
download.microsoft.com/download/7/2/3/723a663c-652a-47ef-a2f5-91842417cab6/Establishing_End_to_End_Trust.pdf
- Northrop, Linda. 2006. *Ultra-Large-Scale Systems: The Software Challenge of the Future*. Software Engineering Institute, Carnegie Mellon, Pittsburgh, PA.
- Department of Defense Strategy for Operating in Cyberspace*. July 2011.
- Energy Horizons: United States Air Force Energy S&T Vision 2011-2026*. United States Air Force Chief Scientist (AF/ST) Report. AF/ST-TR-11-01-PR, 31 December 2011.
- F-35 Lightning II Program Briefing*, December 2009, "NTISR Study OMS"

- Future Cyberspace Operating Environment*. Air Force Space Command.
- GAO 12-375. *DoD Supply Chain: Suspect Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms*. GAO Report 12-375, Feb 21, 2012.
- Global Trends 2025: A Transformed World*. The National Intelligence Council. 2008.
- Goldman, Harriett G. and John P. L. Woodward. "Defending Against Advanced Cyber Threats." The MITRE Corporation. 20 January 2008.
- Goodman, Seymour E. and Herbert S. Lin, eds. *Toward a Safer and More Secure Cyberspace*. Washington, DC: The National Academies Press, 2007.
- Gosler, James. "The Digital Dimension." *Transforming U.S. Intelligence*. Eds. Jennifer Sims and Burton Gerber. Washington, DC: Georgetown University Press, 2005. 96-114.
- Government Accountability Office (GAO) report on Defense Critical Infrastructure*, October 2009.
- Jabbour, K. and Muccio, S. "The Science of Mission Assurance", *Journal of Strategic Security*, vol. IV, no. 2, summer 2011, pp. 61-74.
- Joint Operating Environment (JOE)*. 2010. U.S. Joint Forces Command.
- Joint Operational Access Concept (JOAC)*. V1.0, 17 January 2012. Department of Defense.
- Joint Strategy Assessment 2008-2028*. Defense Intelligence Agency.
- Joint Publication JP 3-12 *Cyberspace Operations* Final Coordination. 10 April 2012.
- Joint Publication JP 3-13, *Information Operations*, 13 February 2006, GL-9, http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf.
- Lee, E. A. and Seshia, S. A, *Introduction to Embedded Systems - A Cyber-Physical Systems Approach*. LeeSeshia.org, ISBN 978-0-557-70857-4, 2011.
- Maybury, M., Chase, P., Cheikes, B., Brackney, D., Matzner, S., Hetherington, T., Wood, B., Sibley, C., Marin, J., Longstaff, T., Spitzner, L., Haile, J., Copeland, J. and Lewandowski, S. 2005. *Analysis and Detection of Malicious Insiders*. In 2005 International Conference on Intelligence Analysis, Sheraton Premiere, McLean, VA.
- McConnell, J. Michael (Director of National Intelligence). "Unclassified Statement for the Record from Testimony on Intelligence Community Annual Threat Assessment before Senate Armed Services Committee." Washington, DC. 27 Feb 2008. http://www.dni.gov/testimonies/20080227_testimony.pdf
- Mission Impact of Foreign Influence on DoD Software*. Washington, DC. Sep 2007. www.acq.osd.mil/dsb/reports/2007-09-Mission_Impact_of_Foreign_Influence_on_DoD_Software.pdf
- National Security Strategy*, May 2010. President of the United States.
- NASIC System Threat Assessment Report*, Aug 2009, "Global Hawk".
- NASIC System Threat Assessment Report*, January 2011, "MQ-9A Reaper".
- NSA Information Assurance Directorate, 13 July 2010, "Operational Security Doctrine for the F-35 KOV-32 Data Security Module"

NSA Information Assurance Directorate, 13 July 2010, “Operational Security Doctrine for the KOV-35 and KOV-35A Communication, Navigation, Identification, Processors (CNIP)”

Owens, W., Dam, K. W. and Lin, H. S (eds) 2009. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Committee on Offensive Information Warfare, Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences, National Research Council.

Quadrennial Defense Review (QDR). 2010

Report of the Defense Science Board Task Force on High Performance Microchip Supply, February 2005. DTIC Report ADA435563.

Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology, March 2009. DTIC Report ADA498375.

Technology Horizons: A Vision for Air Force Science & Technology 2010-2030. Volume 1. United States Air Force Chief Scientist (AF/ST) Report. AF/ST-TR-10-01-PR, 15 May 2010.

“Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program”. The White House Office of Science Technology and Policy. December 2011.

United States Air Force Strategic Environmental Assessment (SEA) 2010-2030. March 11, 2011. Directorate of Strategic Planning, Headquarters, United States Air Force (AF/A8X) 1070 Air Force Pentagon, Washington, DC 20330-1070.

“Worldwide Threat Assessment of the United States Intelligence Community for the House Permanent Select Committee on Intelligence - Unclassified Statement for the Record” Director of National Intelligence. 2 February 2012.

“World Economic Outlook”, International Monetary Fund. April 2011.

Appendix A: Acronyms

ADS-B/C	Automatic Dependent Surveillance-Broadcast/Contract
AF	Air Force
AF SAB	Air Force Scientific Advisory Board
AFMC	Air Force Materiel Command
AFLCMC	Air Force Life Cycle Management Center
AFRL	Air Force Research Laboratory
AFSPC	Air Force Space Command
AMC	Air Mobility Command
AOC	Air Operations Center
APT	Advanced Persistent Threat
ASC	Aeronautical Systems Center
ASD (R&E)	Assistant Secretary of Defense for Research and Engineering
ATC	Air Traffic Control
AWACS	Airborne Warning and Control System
BDA	Battle Damage Assessment
BLOS	Beyond Line of Sight
CAOC	Combined Air Operations Center
CAVE	Cyber Assessment and Vulnerability Evaluations
CMOS	Complementary Metal Oxide Semiconductor
COTS	Commercial Off-The-Shelf
C&A	Certification and Accreditation
CNE	Computer Network Exploitation
CAF	Combat Air Forces
C2	Command and Control
C2 and ISR	Command, Control, Intelligence, Surveillance and Reconnaissance
CONOPS	concept of operations
D2D	Data to Decisions
DARPA	Defense Advanced Research Projects Agency
DCIS	Data Confidentiality & Integrity Systems
DCO	Defensive Cyberspace Operations
DCGS	Distributed Common Ground System
DGO	DoD Global Information Grid Operations
DIACAP	DoD Information Assurance Certification and Accreditation Process
DIB	Defense Industrial Base
DINO	DoD Information Networks Operation
DoD	Department of Defense
DOE	Department of Energy
DON	Department of Navy
DSB	Defense Science Board
DT&E	Developmental Test and Evaluation
DV	Distinguished Visitor
ESC	Electronic Systems Center
FAA	Federal Aviation Administration
FFRDC	Federally Funded Research and Development Center
FOSS	Free and Open Source Software
FPGA	Field-Programmable Gate Array
FLOP	FLoating-point OPeration

FME	Foreign Military Exploitation
GIG	Global Information Grid
GPS	Global Positioning System
HAF	Headquarters Air Force
HBSS	Host Based Security System
IC	Intelligence Community
ICS	Industrial Control Systems
INL	Idaho National Laboratory
IOC	Initial Operational Clearance
IOP	Information Operations Platform
IPT	Integrated Product Team
IR&D	Independent Research and Development
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology
ITV	In-Transit Visibility
ITAR	International Traffic in Arms Regulations
JCTD	Joint Concept Technology Demonstration
JOAC	Joint Operational Access Concept
JSF	Joint Strike Fighter
JSpOC	Joint Space Operations Center
JSTARS	Joint Surveillance and Target Attack Radar System
JTAC	Joint Terminal Attack Controller
ICS	Industrial Control System
KPP	Key Performance Parameter
LIDAR	Light Detection And Ranging
LEO	Low Earth Orbiting
LRE	Launch and Recovery Element
MAJCOM	Major Command
MAF	Mobility Air Forces
MEF	Mission Essential Function
MIMO	Multiple-In Multiple-Out
MIT	Massachusetts Institute of Technology
MOBs	Main Operational Base
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NIU	Network Interface Unit
NREL	National Renewable Energy Laboratory
NSA	National Security Agency
NSF	National Science Foundation
NSS	National Security Space
OCO	Offensive Cyberspace Operations
OFP	Operating Flight Program
OSTP	White House Office of Science and Technology Policy
OT&E	Operational Test and Evaluation
PIT, Platform IT	Platform Information Technology
PMA	Portable Maintenance Aid
PSC	Priority Steering Council
QKD	quantum key distribution

qubits	quantum bit
R&D	Research & Development
RI	AFRL Information Directorate
RF	Radio Frequency
RFI	Request for Information
RFID	Radio-frequency identification
RFP	Request for Proposal
RPA	Remotely Piloted Aircraft
SA	Situational Awareness
SAF	Secretary of the Air Force
SCADA	Supervisory Control and Data Acquisition systems
SDR	Software Defined Radio
SIGINT	Signals Intelligence
SOF	Special Operations Forces
S&T	Science and Technology
S&TI	Scientific and Technical Intelligence
SMC	The Space and Missile Systems Center
SSA	Space Situational Awareness
STAR	System Threat Assessment Report
STEM	Science, Technology, Engineering and Mathematics
SWAP	Size, Weight and Power
TACC	Tanker Airlift Control Center
TCAS	Traffic Collision Avoidance System
T&E	Test and Evaluation
TRL	Technology Readiness Level
TSAT	Transformational Satellite Communications
TTPs	Tactics, Training, and Procedures
TTCP	The Technical Cooperation Program
UAV	Unmanned Air Vehicle
U.S.	United States
USAF	United States Air Force
USCYBERCOM	United States Cyber Command
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
VLSI	Very-Large-Scale Integration
WAMI	Wide Area Motion Imagery

Appendix B: Terms and Definitions

Additional definitions of more common military terminology are available in the DoD Dictionary of Military Terms, http://www.dtic.mil/doctrine/dod_dictionary

Agility. Nimbleness and adaptability. (For example, agility can be enabled by dynamic, reconfigurable architectures such as IP hopping at the network layer.)

Antiaccess (A2). Those capabilities, usually long-range, designed to prevent an advancing enemy from entering an operational area. *Joint Operational Access Concept (JOAC)*.

Area-Denial (AD). Those capabilities, usually of shorter range, designed not to keep the enemy out but to limit his freedom of action within the operational area. JOAC.

Assured Access. The unhindered national use of the global commons and select sovereign territory, waters, airspace and cyberspace, achieved by projecting all the elements of national power. JOAC.

Cloud Computing. Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models. The five essential characteristics are on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. The three service models are Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), and Cloud Infrastructure as a Service (IaaS). The four deployment models are Private Cloud, Community Cloud, Public Cloud, and Hybrid Cloud. (Source http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf)

Command and Control (C2). The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. JP 1.

Cyberspace.

1. Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures and associated data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. JP1-02.
2. Domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. [“Joint Terminology for Cyberspace Operations”, VCJCS memo for the Service chiefs, combatant commanders and directors of Joint Staff directorates, undated.]

3. Cyberspace is a domain that requires man-made technology to enter and exploit. The only difference is that it is easier to see and sense the other domains. As with air and space, effects of cyberspace operations can occur simultaneously in many places. They can be precise, broad, enduring, and transitory. AFDD 3-12

Cyberspace Capability. A device, computer program, or technique, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace. JP 3-12.

Cyberspace Operations (CO). The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. JP 3-12.

Cyberspace Security. Assured access to cyber systems and services preserving confidentiality, integrity, and availability to reliably provide robust and resilient capabilities that meet operational needs.

Cyberspace Situational Awareness (CSA). The requisite current and predictive knowledge of the cyberspace environment and the operational environment upon which cyber operations depend - including physical, virtual, and human domains - as well as associated threats, vulnerabilities, and dependencies - as well as all factors, activities, and events of friendly and adversary cyber forces across the spectrum of conflict.

Deception. Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce the enemy to react in a manner prejudicial to the enemy's interests. See also military deception—Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.

Domain Superiority. That degree of dominance of one force over another in a domain that permits the conduct of operations by the former at a given time and place without prohibitive interference by the latter. JOAC.

Defensive Cyberspace Operations (DCO). Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data networks, and net-centric capabilities. Also called DCO. JP 1-02.

Department of Defense information network operations. Operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance of the Department of Defense information networks. (Definition will be included in JP 1-02 upon approval of JP 3-12)

Electromagnetic Deception. The deliberate radiation, re-radiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or to enemy electromagnetic-dependent weapons, thereby degrading or neutralizing the enemy's combat capability.

Electromagnetic Spectrum. The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. JP 3-13.1

Electronic Attack (EA). Division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. JP 3-13.1

Electronic Warfare (EW). Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. JP 3-13.1

Fast Follower. A fast follower rapidly adopts and/or, as needed, adapts and/or accelerates technologies originating from external organizations that are leaders in and make major investments in focused S&T areas as their primary mission. An example of this would be microgrids in which DOE, the national laboratories, and utilities have significant expertise and investments. In some areas where the Air Force is in general a fast follower, there might be niches or mission specific requirements that require focused Air Force investments to ensure leadership (e.g., hardening microgrids, on-board SWAP sensitive operations).

Force Protection (FP). Preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease. JP 3-0.

Full-spectrum Superiority. The cumulative effect of dominance in the air, land, maritime, and space domains and information environment (which includes cyberspace) that permits the conduct of joint operations without effective opposition or prohibitive interference. JP 3-0.

Incident.

1. In information operations, an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent. JP 3-28.
2. An occurrence, caused by either human action or natural phenomena, that requires action to prevent or minimize loss of life or damage to property and/or natural resources. See also information operations. JP 3-28.
3. An occurrence that A) jeopardizes the, confidentiality, integrity or availability of information or an information system; or B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.'

Information Environment. The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. JP 3-13.

Information Operations (IO). The integrated employment, during military operations, of information related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. SecDef Memo 12401-10, SC and IO in the DoD. 25 Jan 2011. See also JP 3-13.

Information Security. protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—“(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring nonrepudiation and authenticity; “(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and “(C) availability, which means ensuring timely and reliable access to and use of information.

Information Superiority. The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. See also information operations. JP 3-13.

Information System. The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. JP 3-13. (This term and its definition modifies the existing term and definition and is approved for inclusion in the next edition of Joint Pub 1-02.)

Insider Threat. A person, known or suspected, who uses their authorized access to Department of Defense facilities, systems, equipment, information or infrastructure to damage, disrupt operations, commit espionage on behalf of a foreign intelligence entity or support international terrorist organizations. JP 2-01.2

Military Deception (MILDEC). Actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. JP 3-13.4

Mission Assurance (cyberspace). Measures required to accomplish essential objectives of missions in a contested environment. Mission assurance entails prioritizing mission essential functions, mapping mission dependence on cyberspace, identifying vulnerabilities, and mitigating risk of known vulnerabilities. AFDD 3-12.

Movement and Maneuver. This joint function encompasses disposing joint forces to conduct campaigns, major operations, and other contingencies by securing positional advantages before combat operations commence and by exploiting tactical success to achieve operational and strategic objectives. This function includes moving or deploying forces into an operational area and conducting maneuver to operational depths for offensive and defensive purposes. It also includes assuring the mobility of friendly forces. [Alt: A movement to place ships, aircraft, or land forces in a position of advantage over the enemy. JP 3-0.]

Offensive Cyberspace Operations (OCO). Operations conducted to project power against adversaries in or through cyberspace. Also called OCO. (Definition will be updated in JP 1-02 upon approval of JP 3-12)

Operations Security (OPSEC). A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities. JP 3-13.3

Power Projection. The ability of a nation to apply all or some of its elements of national power - political, economic, informational, or military - to rapidly and effectively deploy and sustain forces in and from multiple dispersed locations to respond to crises, to contribute to deterrence, and to enhance regional stability. JP 3-35

Protection. Preservation of the effectiveness and survivability of mission related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area. JP 3-0

Resilience. The ability to avoid (or deflect or absorb), 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). (Resilience can be enabled by redundancy, diversity, and fractionation (distributed functionality) which allow systems to repel, absorb, and/or recover from attacks. Resilience can be enhanced through 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.)

Reachback. The process of obtaining products, services, and applications, or forces, or equipment, or materiel from organizations that are not forward deployed. JP 3-30.

Space. A medium like the land, sea, and air within which military activities shall be conducted to achieve U.S. national security objectives.

Space Situational Awareness (SSA). The requisite current and predictive knowledge of the space environment and the operational environment upon which space operations depend - including physical, virtual, and human domains - as well as all factors, activities, and events of friendly and adversary space forces across the spectrum of conflict. JP 3-14.

Technology Leader. A technology leader creates or invents novel technologies through research, development and demonstration. Examples of areas in which the Air Force is a technology leader include provide defensive cyber operations for aviation missions.

Technology Watcher. A technology watcher uses and leverages others S&T investments in areas that are not a primary or core mission. For example, in terms of commodity hardware and software, the Air Force might use but not develop certain mission supporting information services.

Title 10. Portion of the United States Code that contains the organic law governing the Armed Forces of the United States and provides for the organization of the Department of Defense, including the military departments and the reserve components, and the organization, training, and equipping of forces.

Title 18. Portion of the United States Code that provides the criminal penal code and procedure for the federal government and is applicable to Air Force law enforcement activities.

Title 32. Portion of the United States Code that is a compilation of federal laws pertaining to the militia, National Guard, the Army National Guard of the United States, and the Air National Guard of the United States.

Title 50. Portion of the United States Code that establishes the Council of National Defense for the coordination of industries and resources for national security and welfare, and includes authorities related to foreign intelligence surveillance.

Appendix C: Cyber Vision 2025 Team and Senior Independent Expert Reviewer Group

The following individuals played instrumental roles in advancing the Air Force Cyberspace S&T vision and strategy:

■ Executive Leadership

- Honorable Michael B. Donley (SAF/OS), Secretary of the U.S. Air Force
- General Norton A. Schwartz (AF/CC), 19th Chief of Staff of the U.S. Air Force
- General Mark Welsh, (AF/CC), 20th Chief of Staff of the U.S. Air Force
- Honorable Erin C. Conaton (SAF/US), Undersecretary of the U.S. Air Force
- General Philip M. Breedlove (AF/VC), Vice Chief of Staff
- Gen William Shelton (AFSPC/CC), Space Command Commander and Cyberspace Superiority Core Function Lead Integrator

■ Senior Governance Team

- Dr. Mark Maybury (Chair) (AF/ST), Chief Scientist of the U.S. Air Force
- Lt Gen Mike Basla (AFSPC/CV then SAF/CIO A6) - transferred positions at end of study
- Lt Gen Larry James (AF/A2)
- Lt Gen William Lord (SAF/CIO A6)
- Lt Gen Chris Miller (AF/A8)
- Lt Gen Janet Wolfenbarger (AF/AQ)

■ Key Stakeholders

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

■ Cyberspace 2025 Mission Area Study Leads, Co-Leads and Key Members

- Air: Dr. Kamal Jabbour (AFRL/RI), Dr. Donald Erbschloe, (AMC/ST), Mr. William Marion (ACC/CTO), Ward Walker (AMC/CTO), Todd Humiston (AFRL/RITC)
- Space: Dr. Doug Beason (AFSPC), Dr. Jim Riker (AFRL/RV) (vice), Dr. Roberta Ewart (SMC/XR), & Col Brad Buxton (SMC)
- Cyber: Dr. Rich Linderman (AFRL/RI), Dr. Doug Beason (AFSPC), Mr. Arthur Wachdorf (24AF), Ms. Emily Krzysiak (AFRL/RIB), and Mr. Mike Kretzer (688th)
- C2 and ISR: Dr. Steven K. Rogers (AFRL/RV/RI), Dr. Rick Raines (CCR, AFCyTCoE) (vice), Dr. Chris Yeaw (AFGSC), Mr. Ron Mason (ESC), Mr. Stan Newberry (AFC2IC), B Gen Scott Bethel (AFISRA/CV), B Gen (S) John Bansemer (AFISRA/CVA), DISL Keith Hoffman (NASIC), Col “Rabbi” Harasimowicz, (70 ISRW), John Vona (AFC2IC), Tom Clark (AFRL/RISB), Carla Hess (AFRL/RIBA)
- Mission Support (Acquisition, Test & Evaluation, Education & Training, 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), Mr. David Wascak (NASIC), Col Matthew Hurley (AF/A2DD)
- Study Administration, Management and Leadership: Col Rod Miller (AF/ST)
- Study Support: Penny Ellis (AF/ST)

■ **Additional Subject Matter Experts, Focal Points, and Partners:**

- Gen "Ed" Wilson (AFCYBERCOM), Mr. Randall Walden (SAF/AQI), MG Biscone (STRATCOM), Mr. Jerry Gandy (STRATCOM/A9), BG Mark Westergren (AF/A2D – ISR), Dr. Mark Gallagher (A9), Mr Robert De Mayo (AF/A2CS), Dr. Brian Kent (AFRL/RV), Dr. Morley Stone (AFRL/RH), Dr. Jack Blackhurst (AFRL/RH), Bob Herklotz (AFOSR), Rich White (67th), Deputy Robin "Montana" Williams (57th IWAS CC), Lt Col BethAnn Shick (SMC/SYFY), Linda Millis (DNI, Private Sector Partnerships), Col Rex R. Kiziah (AFSPC/ST), Col Brent A. Richert (USAF/DFER), Maj Iqbal Sayeed (AFGSC/A4/7), Mr. Cameron Stanley (SAF/IE)

■ **Senior Independent Expert Review Group**

• **Air:**

- Prof Mark Lewis³, University of Maryland
- Ms. Natalie Crawford⁶, Senior Fellow, RAND
- Lt Gen George Muellner⁶, (Ret) USAF
- Mr. Robert Osborne, NNSA

• **Space**

- Dr. Mike Yarymovych^{3, 6}, President Sarasota Space Associates
- Don Kerr²
- Mr. Keith Hall², Booz Allen Hamilton
- Dr. Rami Razouk⁶, Senior Vice President, Aerospace
- Mr. Matt Linton, NASA ARC-IS

• **Cyber**

- Prof Ed Feigenbaum³, Stanford
- Gil Vega, DOE
- Prof. Gene Spafford, Purdue
- Dr. Herb Lin, Chief Scientist, Computer Science and Telecommunications Board, National Research Council of the National Academies
- Mr. Andrew Makridis, CIA
- Mr. Glenn Gafney, CIA
- Dr. Paul Nielsen, Director and CEO, Software Engineering Institute
- Dr. Marc A. Zissman MIT LL
- Mrs. Harriet Goldman, MITRE
- Gen Mike Hayden¹ (Ret), USAF
- Lt Gen Ken Minihan⁴ (Ret), USAF
- RADM Will Metts, NSA/TAO
- Paul Laugesen, NSA/TAO
- Dr. Yul Williams, NSA/CSS TOC
- David J. Mountain, Advanced Computing Systems Research Program, NSA Research Directorate
- Dr Starnes Walker, FltCyber, Navy
- Tim Grance, NIST

• **C2 and ISR**

- Prof Alex Levis³, GMU
- John Woodward, MITRE
- Sue Lee Short, JHU-APL
- VADM Mike McConnell¹, (Ret) USN
- Lt Gen David Deptula, (Ret) USAF
- Lt Gen Ted Bowlds, (Ret) USAF

- Lt Gen Robert Elder, (Ret) USAF
- **Mission Support**
 - Mr. Mike Aimone, Director, OSD AT&L
 - John Gilligan⁵
 - Jim Gosler, Sandia
 - Lt Col Marion Grant, USCYBERCOM/J9
 - Giorgio Bertoli, Army
 - Dr. Ernest McDuffie , CMU
 - Mike Aimone, OSD (I&E)
 - Lt Gen (Ret) Trey Obering, USAF
 - Dr. Tim Persons, GAO
- **Enabling Science and Technology**
 - Prof. Werner Dahm³, Director Security & Defense Systems Initiative (SDSI), Arizona State Univ
 - Charles Bouldin, NSF
 - Lauren M. Van Wazer, OSTP
 - Tomas Vagoun, NITRD
 - Konrad Vesey, IARPA
 - Stan Chincheck, NRL
 - Dr. Wen C. Masters, ONR
 - Gen (Ret) Jim McCarthy, USAFA
 - Dr. Peter Friedland, formerly NASA, AFOSR Advisor
 - Prof. Patrick H. Winston, MIT
 - Dr. David Honey, DNI
 - Dr. Steven King, OSD(R&E) PSC
- **Coalition**
 - Group Cpt Andrew Gudgeon, UK
 - Dr. Brian.Hanlon. DSTO, Australia
 - Joseph Templin, Canada

Notes:

¹Former Director of National Intelligence

²Former Director of the National Reconnaissance Office

³Former Chief Scientist of the USAF

⁴Former Director of NSA and DIA

⁵Former AF Chief Information Officer

⁶AF SAB Executive Committee

Appendix D: Cyber Vision 2025 Working Meetings

A series of Air Force mission focused working meetings were held to shape the S&T strategy. Wherever possible, these were collocated with mission operations to facilitate direct engagement with operational communities. In addition, to maximize input from and engagement with the best talent and ideas from the national laboratories, industry, academia and non profits, an RFI's were issued enabling multiple security levels of response, resulting in hundreds of ideas which were carefully reviewed and selected for presentation at various summits.

- 18-20 Jan – Initial Air-Cyber Mission Meeting – Edwards AFB
Lead: Dr. Kamal Jabbour, Host: AFOTEC, AFFTC
- 23 January – Threat Workshop (SCI), Washington, DC
 - Lead: Mr. Gary O'Connell (Chief Scientist NASIC) Host: MITRE
- 24 Feb – RFI Input Due (See www.tinyurl.com/cybervision)
- 8-9 Feb - Air-cyber: 8 Feb (Scott AFB), 9 Feb (Langley)
Leads: Dr. Kamal Jabbour (AFRL/RI), Dr. Don Erbschloe (AFMC), Bill Marion (ACC).
Host: 8 Feb (Scott AFB), 9 Feb (Langley)
- 29 Feb – 2 Mar – West Coast Industry Visit for team leads
- 12-13 March – Air Workshop, Langley
Leads: Dr. Kamal Jabbour (AFRL/RI), Dr. Don Erbschloe (AMC),
Mr. Bill Marion (ACC)
- 14-15 March – C2 and ISR Workshop, Langley
Leads: Dr. Steven K. Rogers (AFRL/Ry), Mr. Ron Mason (ESC), Mr. Stan Newberry (AFC2IC), Dr. Chris Yeaw (AFGSC/ST), B Gen Scott Bethel (AFISRA/CV), B Gen (S) John Bansemer (AFISRA/CVA), DISL Keith Hoffman (NASIC), Dr. Rick Raines (AFIT/CCTE)
- 19-21 March – Space-Cyber, Cyber, S&T Workshops @ AFSPC, Peterson AFB
Leads: Dr. Douglas Beason (Chief Scientist, AFSPC), Dr. Rich Linderman (Chief Scientist AFRL/RI), Dr. Jennifer Ricklin (Chief Technologist AFRL)
- 27 March - Mission Support Summit, DC
Leads: Dr. Steve Walker, SAF/AQR, Maj Gen Tom Andersen (LeMay Center),
Mr. Mike Kretzer (688th), Dr. Nathaniel Davis (AFIT)
- 28 March - AF-DoE Cyber Summit, ORNL
Leads: Dr. Mark Maybury (AF/ST), Dr. Christopher Yeaw (AFGSC/ST), Mr. Mike Aimone (OSD AT&L), Dr. Steven K. Rogers (AFRL/Ry)
- April @DARPA - DARPA Cyber PM Briefs to CV25 Mission Leads
- 10 April @SAFTAS - Senior Independent Expert Review Group – Presentation Review
- 9 May @SAFTAS - Senior Independent Expert Review Group – Document Review
- June 2012 Presentation at CORONA
- 15 July 2012 Presentation to SecAF and CSAF

Several cyber related events occurred during this time period including:

- 7-9 Feb, AFCEA Cyber Conf, Colorado Springs
- 5-9 March – AFOSR Computational Sciences Review, DC
- 22-23 March – AFA Cyber Futures Conference, Gaylord, DC

Appendix E: Cyber Vision 2025 Terms of Reference

Background

An Air Force wide Cyber S&T vision is needed to articulate a path forward that will enhance our ability to forecast future threats, mitigate vulnerabilities, enhance the industrial base, and develop the operational capabilities and cyber workforce necessary to assure cyber across all Air Force mission areas. This effort will not establish policy or formulate requirements. Rather it aims to create an integrated, Air Force-wide, near-, mid-, and long-term S&T vision that supports core Air Force missions and, where possible, creates revolutionary cyber capabilities.

Approach

Partnering with air staff, MAJCOMs, and key stakeholders, AF/ST will:

- Identify cyber state of the art and best practices in government and private sector
- Analyze current and forecasted cyber capabilities, threats, vulnerabilities, and consequences (e.g., robustness, resilience, readiness) across core AF missions to identify critical S&T gaps
- Articulate an Air Force near (FY11-FY15), mid (FY16-20) and long (FY21-25) term cyber S&T vision (aka “a Cyber S&T Flight Plan”) to fill these gaps, indicating where the Air Force should lead, follow, or watch
- Identify opportunities to leverage and partner other public, private sector and allied capabilities and investments, engaging S&T subject matter experts from within and outside the AF
- Address cyber S&T across all Air Force core missions and functions (air, space, C⁴ISR) in a comprehensive manner which includes policy as well as DOTMLPF considerations.
- Coordinate regularly with AF Cyber leadership and via periodic updates to SAF/US and AF/CV.

Products

- Preliminary cyber S&T vision to SAF/US and AF/CV by 1 June, 2012.
- Final briefing to SAF/OS, AF/CC, SAF/US and AF/CV by 15 July 2012. Publish report by 1 January 2013 articulating cyber S&T gaps, vision, and most promising near-, mid- and long-term vectors.