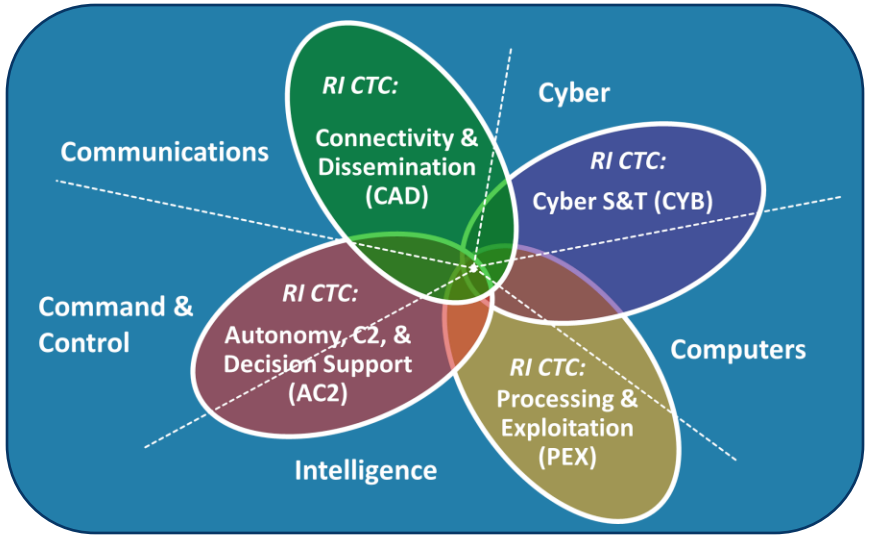
Cyber S&T Core Technical Competency (CTC) Overview

Information Directorate

AFRL/RI Cyber Science & Technology CTC

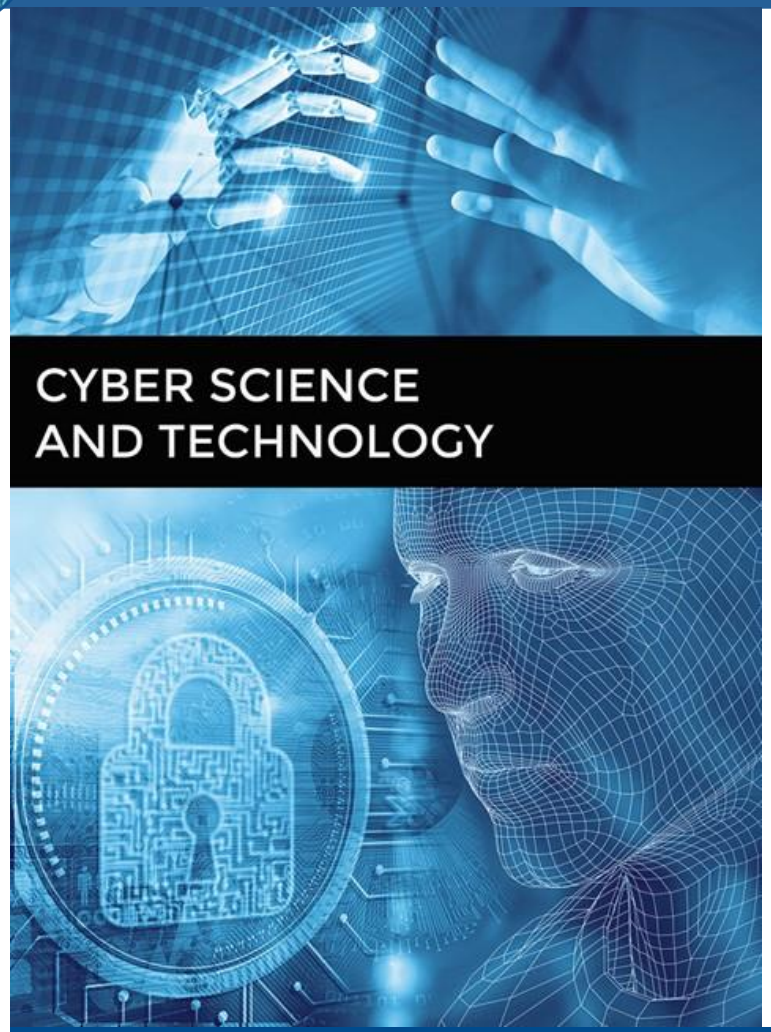
One of the four Core Technical Competencies (CTCs) that comprise the mission space for the Air Force Research Laboratory (AFRL) Information Directorate (AFRL/RI)

- **AC2 (RIS)**: Decision making and command & control with heavy AI/ML emphasis
- **CAD (RIT)**: Networked communications fabric, including RF, IP, quantum, etc.
- **CYB (RIG)**: Offensive and defensive cyber operations and cyber assurance
- **PEX (RIE)**: Processing and transforming big data into information



Technologies that enable our freedom to operate in cyberspace, while denying the adversary the same

Cyber Science & Technology CTC Fundamentals



Mission: Deliver the science and technology necessary to ensure cyberspace superiority and support the conduct of full-spectrum, multi-domain, integrated cyberspace operations.

Vision: An Air Force equipped with technologies that enable our freedom to operate in cyberspace while denying the adversary the same.

CORE PRINCIPLES

Context is essential to R&D	[Scope]
Evidence as a first principle of research	[Effectiveness]
Cyber is driven by mission requirements	[Risk]

Mission Assurance as first priority

Leveraging the Cyber Domain to the Nation's Advantage

Air Force Strategy

- **Assuring Information as it Traverses Mission Infrastructure, Supporting Operations in All Domains**
- **Projecting Power In, Through and From Cyberspace as a Domain**
  - Cyber Operations, Air Enabled (COAE)
  - Counter Adversary Defense Systems
  - Joint Intelligence Preparation of the Operational Environment
- **Integrate, Synchronize, and Optimize Cyber Operations Across Domains in Order to Compete and Deter**

Air Force Operational Imperatives

1. **Defining Resilient Space Order of Battle and Architectures (defensive and offensive).**
2. Achieving Operationally-Optimized Advanced Battle Management System (ABMS) / Air Force Joint All Domain Command and Control (JADC2).
3. Achieving Moving Target Indication and Tracking at Scale (air, sea surface and ground mobile targets).
4. **Defining the Next Generation Air Dominance System of Systems (sensors, communications, command & control, weapons, and uncrewed aerial vehicles).**
5. **Defining Optimized Resilient Basing, Sustainment, and Communications in a Contested Environment.**
6. Defining the B-21 Long Range Strike Family of Systems.
7. **Evaluating Readiness of the DAF to Transition to a Wartime Posture Against a Peer Competitor.**

Space Force Strategy

- **Preserving freedom of action in space is the essence of military space power**
- **CORE COMPETENCIES**
  1. Space Security
  2. Combat Power Projection
  3. Space Mobility & Logistics
  4. Information Mobility
  5. Space Domain Awareness

AFRL External Integration and Collaboration

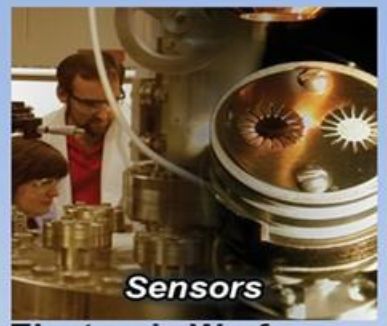
Integration and leadership throughout the user community…

Liaisons, details, Communities of Interest (CoI), staff augmentation

- Office of the Secretary of Defense (OSD)
- 16th Air Force at Joint Base San Antonio-Lackland
- Air Combat Command (ACC)
- Air Force Life Cycle Management Center (AFLCMC)
- Defense Advanced Research Projects Agency (DARPA)

Industry and academia

AFRL Cross-Directorate Cyber Collaborations

RI	711HPW	RY	RV	RW
				
Mission Assurance Command & Control / Visualization Cyber Operations Communications & Networking Processing & Exploitation Signals Intelligence Electronic Protection	Cognitive Task Analyses Operator Selection & Training Adaptive Interfaces / Visualization	Electronic Warfare Avionics Protection	Space System Hardening	Munition Systems Cyber Resiliency

AFRL's Cyberspace Capability Leadership

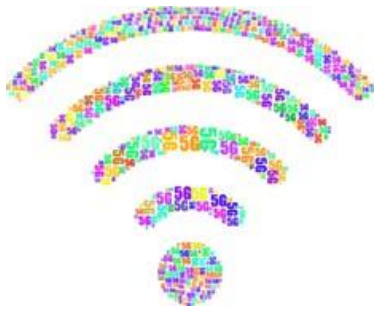
Overarching Cyber Trends of Interest

- **Ubiquity of Cyber**
  - 5G and IoT increase pervasiveness of cyber elements
  - Growth in availability of commercial assets
  - Explosion of available publicly available information (PAI)
- **Increasing Complexity**
  - Disadvantage for cyber assurance/defense
  - Advantage for cyber offense
- **Continued Military Reliance on Commercial Assets**
  - Commercial cloud for storage and processing, routing infrastructure, space assets
  - Commercial components in military systems
- **Increased Functionality within and Reliance on the Space Domain**
  - Expanded network access
  - Mesh networks in space for increased resilience
- **Resource Scarcity Driving Increased Worldwide Conflict**
  - Increased environmental risks and survival stakes shift in deny, delay, disrupt, destroy, or manipulate (D4M) effects
  - Potential increase in attacks with greater visibility/effects

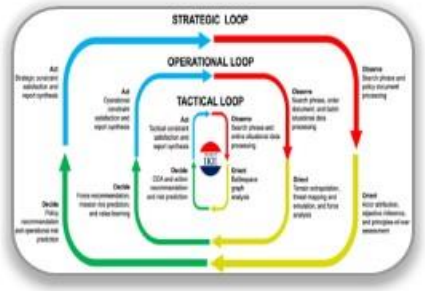
Technological Trends of Interest

- Internet of Things and 5G/6G
- Zero-Trust Architectures
- Agile Development (DevSecOps)
- Autonomy/AI/ML
- Offensive/Defensive Implications of Future Computing Platforms
- Fully Immersive Environments

  (Virtual/Augmented Reality)



Cyber S&T CTC Lines of Effort



Cyber Warfighting

Cyber warfighting technologies that support joint, integrated DCO-OCO-DODIN operations across all domains and levels of conflict. **Vision:** Cyber operations on par and integrated with air and space.

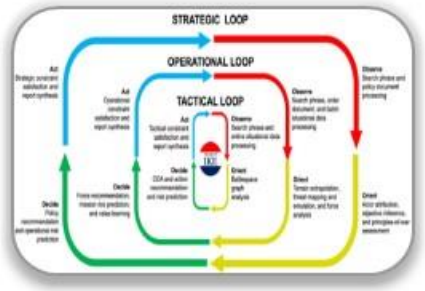
Cyber Assurance

Integrated components and processes that provide measureable and provable guarantees for current and future system architectures. **Vision:** Mission assurance in environments of heterogeneous trust.

EM-Cyber Convergence

Fusion of wired & wireless capabilities with advanced signal processing, enabling future integrated multi-domain ops and emerging missions. **Vision:** Cyber ops agnostic to medium and geography.

Cyber S&T CTC Lines of Effort



Cyber Warfighting

Cyber C2
Cyber Effects
Measurement & Quantification

Data/Domain Models
Decision Support (AI/ML)

Infrastructure | Capabilities | Measurement

Cyber Assurance

Static & Dynamic Analysis
Security Proofs
Cyber Vulnerability Analysis

Software Reasoning
Novel Hardware / Software Features

Hardware | Software | Process

EM-Cyber Convergence

Signal Processing
Optimized Hardware

EM-based Effects
Protocol Analysis

Integration | Analysis | Effects

Cyber S&T CTC Portfolio Activities

Cyber Warfighting

Cyber Assurance

EM-Cyber Convergence

International Partnerships → **India, Estonia, Finland, UK, ROK, Singapore, Australia, Netherlands, Canada**

Community Leadership (e.g. hackfests, academic → **Tech Warrior Ops, Support for CyberX and RED FLAG**

Education → **ACE, Support for UCWT 2.0, IA Fellowship, VICEROY**

In-House & Transition Activities → **RIDER, Firestarter**

Emergent Cyber Challenges

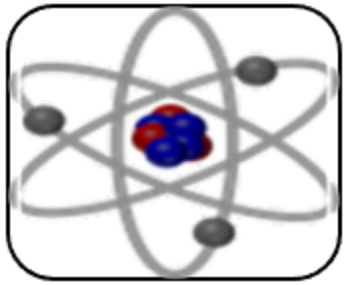
AFRL leads development and employment of future concepts in support of mission assurance concepts

Cyber technologies for emergent environments in FY23 and beyond

- Automated, integrated cyber capabilities
- Security implications of modern systems development practices
- Fundamental concepts for EM-cyber
- Cyber implications to information warfare
- Protocol analysis techniques
- Digital twins of systems for vulnerability analysis

Space-Cyber Applications

Heterogeneous-Trust Concepts



Future Computing Platform Implications

Future UAS Threats

Cyber Workforce Transformation

Recent Transition Activities

Counter-Unmanned Aircraft System Operational Science & Technology Applications (COSTA)

- Ninja C-sUAS S&T innovation – Counter small unmanned aerial vehicles (C-sUAS)
- Transitioning to AFLCMC/HBU with hundreds of Ninja systems fielded to bases around the world

Rapid Cyber Prototyping and Transition (RCPAT)

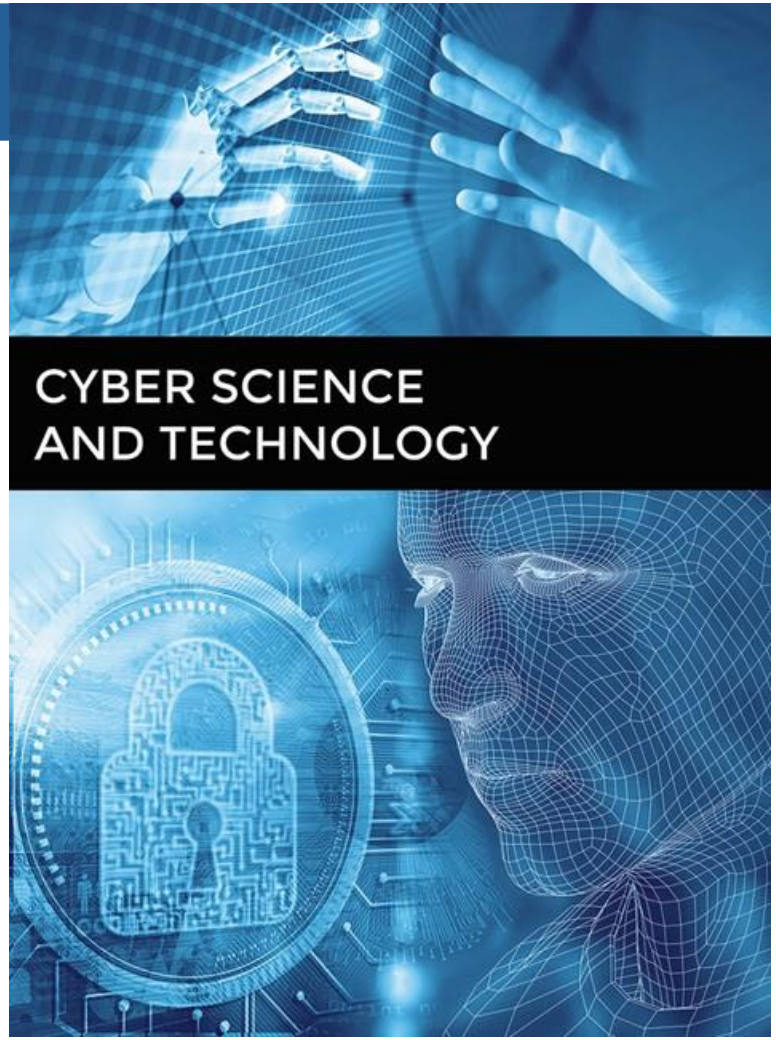
- Firestarter rapidly transitions cyber technologies to the warfighter
- Transitioned dozens of tools to capabilities/organizations such as CVA/H, AFLCMC, 90 COS
- Threat intelligence, cyber ops SA, automated testing, fuzzing, malware analysis

Advanced Course in Engineering Cyber Security Boot Camp (ACE)

- 10-week summer program to educate and train the cyber leaders of tomorrow
- Transitioned OCO/DCO range environment, tabletop cyber exercise, and cryptographic attack infrastructure to support Undergraduate Cyber Warfare Training (UCWT) and impact all AF/SF 17A/B

Summary

- Expansive & diverse portfolio focused on key Air Force, DoD, IC cyber S&T needs
- Integrated into the research & operational communities (fosters research – development – transition cycle)
- Strategy and warfighter requirements → core research areas → transitioned technologies



Contact:

Sonja Glumich | Acting Cyber S&T CTC Lead

Air Force Research Laboratory Information Directorate

Special Programs Division (AFRL/RIZ)

525 Brooks Road, Rome NY 13441

sonja.glumich@us.af.mil

Questions?