AFOSR/Cyber and Information Technology

24 April 2013

Robert J. Bonneau, Ph.D.
Department Chair
AFOSR/RTC
Air Force Research Laboratory

Integrity ★ Service ★ Excellence

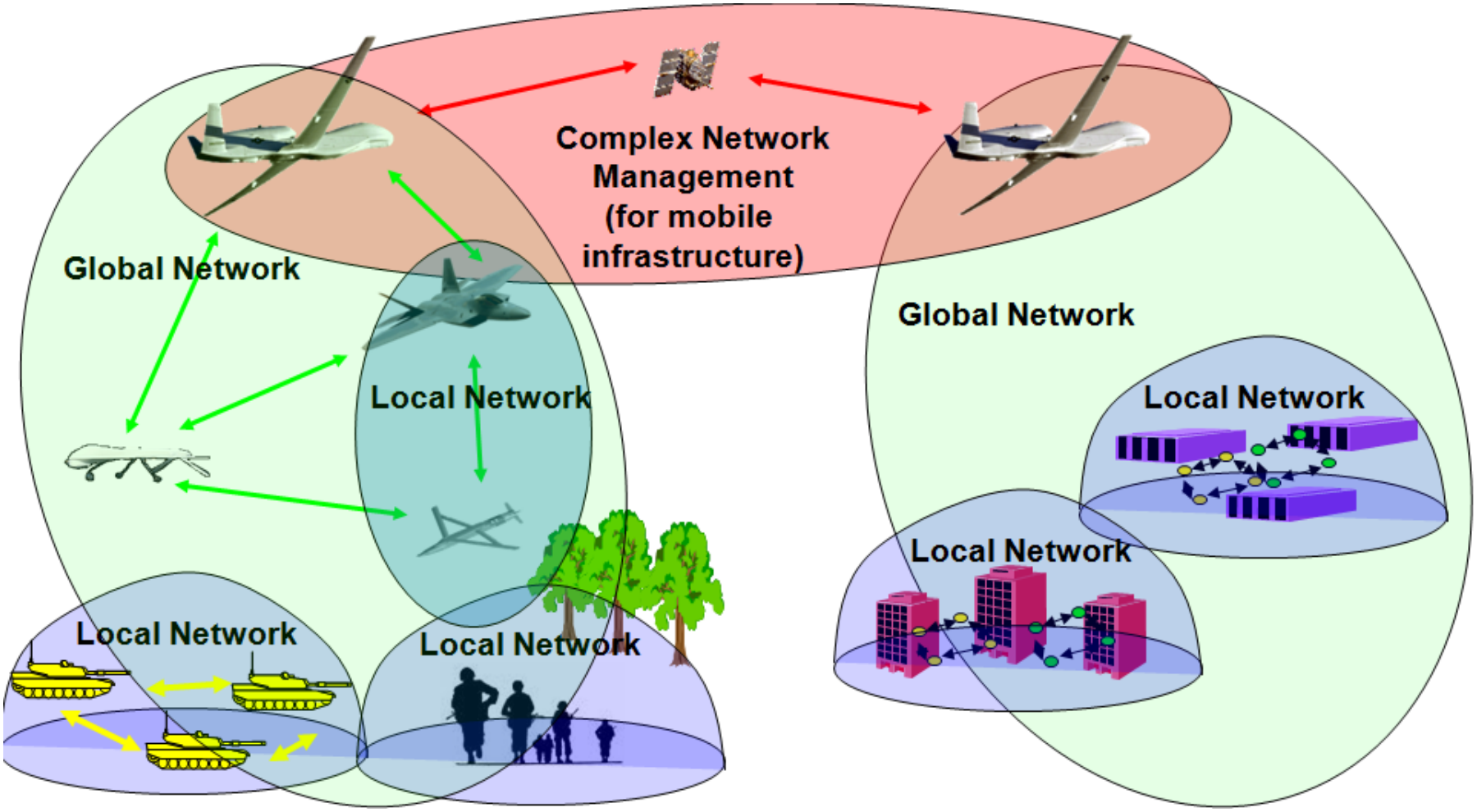
Overview

- Air Force Cyber/Information Environment
- Example Enabling Technologies for Cyber Vision 2025
  - Resilient Future C2 Architectures
  - Human/Machine Risk Assessment & Autonomy
  - ISR Mission Analysis
- Information Technology Transition Process

Air Force Cyber/Information Environment

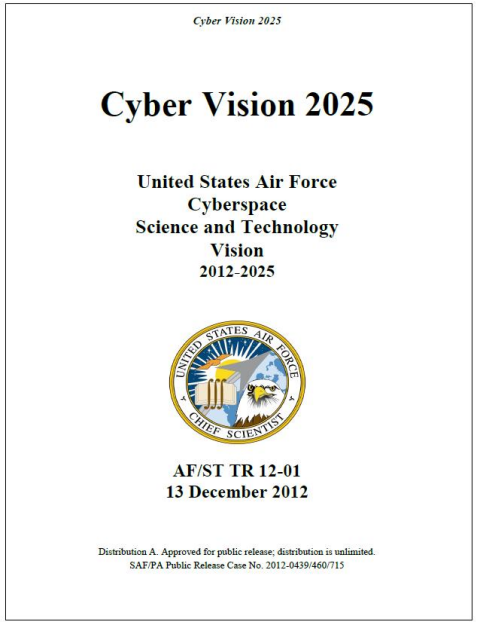
Air Force cyber and C2/ISR missions are distributed often dynamic networked environment

- AFOSR uses advanced mathematics to secure, model, and protect



Enabling Cyber S&T

Fundamental research questions from Cyber Vision 2025 can be addressed through Complex Networks and in AFOSR information science programs.



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

Enabling Technology For Cyber Vision 2025

Area	Near (FY12-FY15)	Mid (FY16-20)	Long (FY21-25)
Foundations	Measurement, Analysis,& Verification	Taxonomy of System Vulnerability	Quantum Methods for Vulnerability Assessment and Security
Agility and Resiliency	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

Areas discussed

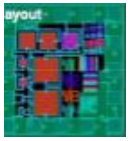
Resilient Future C2 Architectures

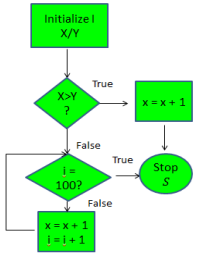
Critical network, software, and hardware states can be measured and verified with optical quantum states.

Measurement Based Verification Enables Automated Code Repair and Risk Quantification

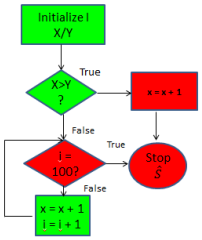
Semiconductor Transmitter

Sender

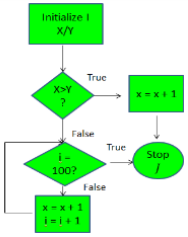




Critical Information Software/Hardware

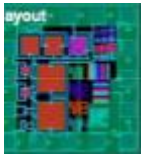


Information Loss/ Compromise



Automated Code Repair/ Recovery/Protection

Receiver

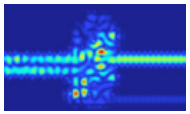


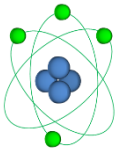
Semiconductor Receiver

Current Systems

Future Quantum Layer

Quantum Transmitter

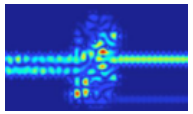




Transmitted Quantum States

Quantum Layer Feedback

Measured Quantum State



Quantum Receiver

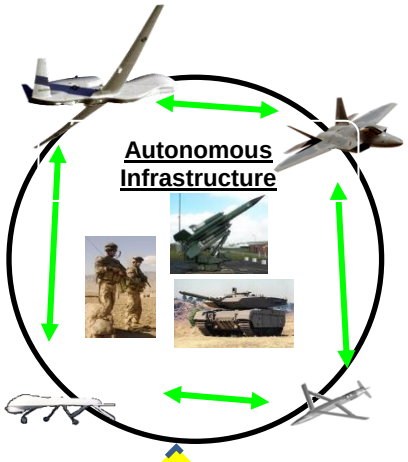
Quantum Verification Enables Instantaneous Physical Layer Analysis/ Protection

Human/Machine Risk Assessment

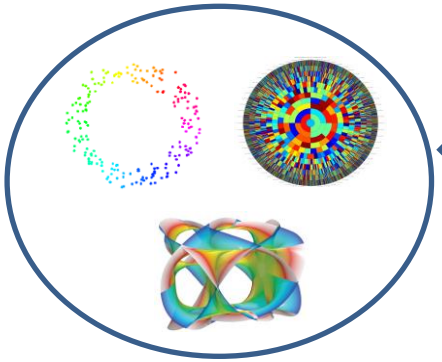
Many problems in cyber and C2/ISR have roots in the autonomy area.

- Missions performed by human vs. machines can be assessed and arbitrated using data-driven risk metrics as conditions evolve.

Partially Autonomous Infrastructure



Real Time Data Analytics



Human Modeling & Sensing

- Natural Language
- User Applications
- Physical Environ.
- Resource Const.
- Cultural Influence
- Social Media
- Social Network

Machine Lower Mission Risk

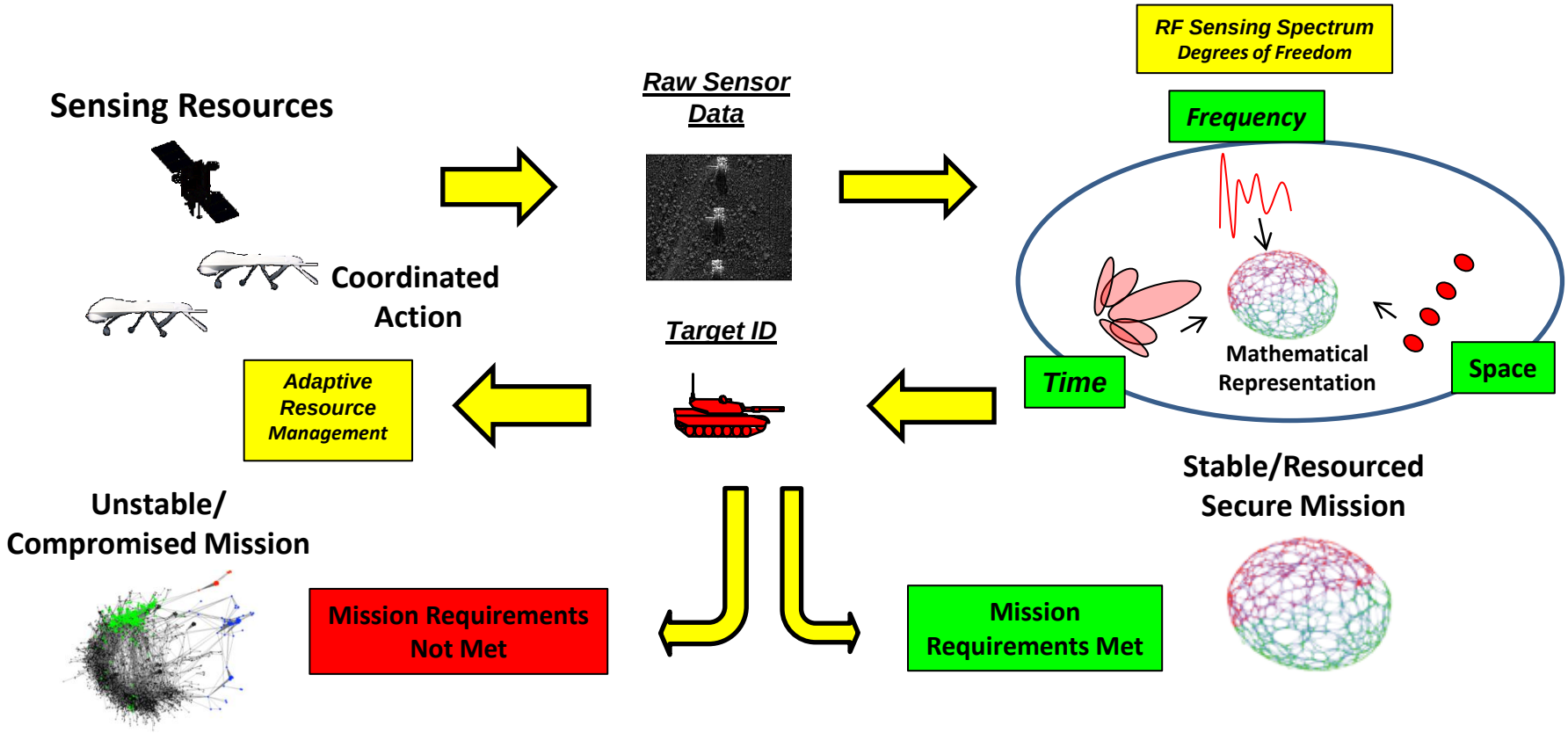
Online Mission Risk Analysis

Human Lower Mission Risk

Mission Requirements & ISR

ISR mission infrastructures are critically dependent on resources such as electromagnetic spectrum to both sense and communicate.

- Automated strategies for spectrum resource allocation must be developed to support higher level mission functions.



Current & Future Architectures & Transition

Introduce measurement algorithms and components into existing systems and future architectures

- **Transition cycles in information technology can be as short as 2-3 years**