Cyberspace: New Frontiers in Technology Insertion

Dr. John S. Bay, ST
Chief Scientist,
Air Force Research Laboratory,
Information Directorate
AFRL Structure

AFRL
Maj Gen C Bedke

Staff
XP

Air Vehicles
Space Vehicles
Information
Munitions
Directed Energy

AFOSR
Materials & Manufacturing
Sensors
Propulsion
Human Effectiveness

Approved for public release; distribution unlimited. Document number Document Number WPAFB 08-2520
Information Exploitation
Information Fusion & Understanding
Information Management
Advanced Computing Architectures
Cyber Operations
Connectivity
Command & Control
DoD Definition: Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated infrastructures.
Some Important Characteristics of Cyber Operations

• Low cost of entry
  – The enemy can be a disgruntled individual with a cheap computer

• Not characterized by physical or geographic boundaries
  – The enemy can be anywhere and everywhere, outside and inside

• R&D and Operations are done in highly classified environment
  – Makes information sharing difficult

• Often relies on exploits that are easily discovered and repaired
  – Sometimes, we only get “one shot”
  – Offense and defense are tightly coupled
  – Technology turnover/refresh
Characteristics of AFCYBER that Catch Our Attention

• Effects, C2, and assessment are to be implemented as integrated capabilities
  – Integrated with other kinetic and non-kinetic capabilities

• The 8th AF capabilities will be organized around an AOC
  – Implies known structure, CONOPs, and doctrine, but only for air and space domains

• The executing authority is the COMAFFOR/JFACC
  – Implies known resources, training, responsibilities, but only for air and space domains

The parity of Cyber with Air and Space domains suggests parallel concepts in C2, battle management, and intelligence technologies
## Cyber Operations Technology Thrusts

<table>
<thead>
<tr>
<th>Thrust</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Access</td>
<td>CYBER</td>
</tr>
<tr>
<td>2. Stealth &amp; Persistence</td>
<td>OFFENSE</td>
</tr>
<tr>
<td>3. Cyber Intelligence</td>
<td>CYBER</td>
</tr>
<tr>
<td>4. Effects (D5) Deny, Disrupt, Degrade, Deceive &amp; Destroy</td>
<td>DEFENSE</td>
</tr>
<tr>
<td>5. Avoid</td>
<td>CYBER</td>
</tr>
<tr>
<td>6. Defeat</td>
<td>DEFENSE</td>
</tr>
<tr>
<td>7. Survive</td>
<td>CYBER</td>
</tr>
<tr>
<td>8. Recover</td>
<td>SUPPORT</td>
</tr>
<tr>
<td>9. Situational Awareness</td>
<td>CYBER</td>
</tr>
<tr>
<td>10. Education</td>
<td>SUPPORT</td>
</tr>
</tbody>
</table>
Warfighting Concepts with a Cyber Twist

- **ATR**
  - What is a “target” in cyberspace?
  - How do we recognize it when we see it?

- **ISR**
  - What sensors can we deploy, and how are these assets shared?

- **EBO/EBA**
  - In cyberspace, the observability of effects is tenuous
  - Second-order effects and cause/effect relationships even more so

- **BDA**
  - Cyber effects propagate in hard-to-detect ways; including in peoples’ behaviors. What is total effect? Can we determine in real-time?

- **AOR**
  - Can cyberspace be sensibly decomposed into manageable combatant commands?

- **SA and PBA**
  - “Situation” is an abstract concept in cyberspace.
  - Visualizations and dynamics (motion, patterns) are ill-defined

- **C2 tools**
  - Can kinetic and cyber tools be controlled with a single toolset?
  - Can kinetic and cyber tools be integrated/synchronized in a single operation?

Approved for public release; distribution unlimited. Document number Document Number WPAFB 08-2520
AFCYBER Key Areas

• FY 07
  – Cyber ORM
  – Software Assurance
  – Critical Infrastructure Identification
  – Offensive Cyber Program Research

• FY08
  – Mission Assurance
  – Security Enhancements (Full CAC compliance)
  – Expanded data encryption (at rest and in transit)
  – Sensitive data offline storage
  – Globally Linked AOCs
  – Offensive Cyber Program Development (Integrated with Air and Space C2)
  – DIB IA

• FY09
  – Expeditionary Networks
  – Counter IO: Data protection
  – IP camouflage
  – Active Defense
  – Critical Infrastructure Protect
  – Boundary monitoring
  – Cyber Control

• FY10
  – Network Survivability
  – Cyber Attack
  – Cyber Interdiction
  – Sensor Disruption
  – C2 Disruption
  – Cyber enabled weapons degradation
  – Electronic Sys Attack (w/ DE)
“Traditional” AFRL Transition

- 6.1 → 6.2 → 6.3, Critical Experiments and Advanced Technology Demonstrations
- Advanced Technology Council

**Lab (☆☆)***
- Identify ATD Candidates
- Budget for Technology Programs
- Develop Transitionable Technologies

**User (☆☆☆)***
- Define Requirements
- Budget Transition Funds

**Center (☆☆☆☆)***
- Interpret Requirements
- Build Transition Program
- Integrate Into Systems
POM-Oriented Transition

**ATD Categories**

- **Category 1:** MAJCOM or Agency supports and has programmed required funding for transition within the FYDP

- **Category 2A:** MAJCOM or Agency supports and is committed to identify transition funding in the next Program Objective Memorandum (POM) cycle or Amended POM

- **Category 2B:** MAJCOM or Agency supports but is not currently able to program for transition funding
Traditional acquisition practices support the development, deployment, and sustainment of long term, highly capable systems

- Focus on minimum risk
- Stable requirements (or a known roadmap)
- Dedicated development and test cycles
- Refined over years based on large body of experience
- 10 year cycle typical for development to transition & Integration
Technology Readiness Levels

- **System Development & Demonstration**
  - TRL 9: Actual system “Flight Proven” through successful mission operations
  - TRL 8: Actual system completed and “flight qualified” through test and demonstration
  - TRL 7: System prototype demonstration in an operational environment
  - TRL 6: System/subsystem model or prototype demonstration in a relevant environment
  - TRL 5: Component and/or breadboard validation in a relevant environment - environment can be simulated
  - TRL 4: Component and/or breadboard validation in a laboratory environment
  - TRL 3: Analytical & experimental critical function and/or characteristic proof-of-concept
  - TRL 2: Technology concept and/or application formulated
  - TRL 1: Basic principles observed and reported

- **Research to Prove Feasibility**
  - TRL 3: Analytical & experimental critical function and/or characteristic proof-of-concept

- **Basic Technology Research**
  - TRL 1: Basic principles observed and reported
The Current Landscape

Bridging The Technology Transition Gap
Source: AFC2ISRC GCIC AFISR ATC

RDT&E

S&T

6.1 Basic Research
6.2 Applied Research
6.3 Adv. Tech Dev
6.4 Program Define/Risk Reduction
6.5 Engr/Manuf Development

Managed by System Program Offices

Tech Base

Managed by AFRL

Applied Technology Council

Means for Tech Transition
Advanced Technology Demo (ATD)
Advanced Concept Tech Demo (ACTD)
Technology Planning IPT
Technical Events (JEFX, CWID etc.)
SPD Initiative
Industry Initiative
Senior Leader Initiative

Emphasis is Necessary on Technology Transition
• Sustained Senior Leader Emphasis
• Continuous Communication
• Integrated Process
• Budget For Production Incorporation

Tech Transition "Seam"
# The S&T Transition Struggle

## Technology Standards

**Strategic**
- Meets Planners Projections
  - General Technology
  - Future Capability
- General Applicability
  - Enhances Performance
  - Foundation (i.e. Open Syst.)
  - Lead Industry
- Expandability – General
- Flexibility – General

## Acquisition Standards

**Tactical**
- Meets User Need
  - Specific Capability
- GOTS/COTS Avail.
- TRL Level Validated
- Production Capable
- Allows COTS Prod. Integration

### Transition Gap

**New Ideas** → **Tech. Push** → **Current Needs**

Approved for public release; distribution unlimited. Document number Document Number WPAFB 08-2520
CYBER Transition Requires new Acquisition Processes

• Cyber Acquisitions may require:
  – Very rapid, urgent fielding needs (days to weeks)
  – Agile development and fielding (months)
  – Traditional development, fielding, and sustainment (months to years) with regular capability “releases” or spirals

• Application to very short cycle times requires alternative approaches
  – Decreased research & development time
  – Limited test and verification
  – “Short tail” logistics

• Strategies to continually innovate and assess
  – Threats and emerging technology,
  – Rapid prototyping
  – Supporting AFCYBER stated capability needs
  – Develop key partnerships

• Migration of some development and assessment efforts to “pre-need” phase
  – Emerging threat R&D strategy to complement reactive acquisition strategy
Full Spectrum Acquisition

Rapid Deployment

Agile/Rapid Acquisition

Traditional Acquisition

Acquisition Dimensions

Urgent

Non-Time Critical

Simple

Complex

Short Lived

Enduring

Stand-Alone

Fully-Integrated

Limited Deployment

Enterprise Deployment

Approved for public release; distribution unlimited. Document number: Document Number WPAFB 08-2520
Alternative Transition Paths

Air Force Research Laboratory

Support to Manufacturing & Industrial Base

Support to Industry Partners

Support to National or International Partners

Technologies Direct to Warfighter

DoD Weapon Systems

Transition

Approved for public release; distribution unlimited. Document number Document Number WPAFB 08-2520
Conclusions: The Changing Battlefield of CyberSpace

“Transition to WHAT?”
Summary

- Rapid research & development strategies
- Constant reassessment of changing landscape resulting in short duration R&D efforts and rapid technology transition
- New acquisition strategies required
- New relationship between research and acquisition
- Innovative challenges/opportunities for community to develop a responsive cyber research and development strategy to work with a full spectrum acquisition capability
- AFRL/RI to lead R&D for the cyber big “A” team
Questions?
The Battle in Cyberspace

Offense, Defense, Infrastructure Elements

Lt Gen Bob Elder