Applying Quantifying Methods to Improve Cyber Security Risk Mitigation Selections for Aircraft

7 March 2018
Roger Beard, CISSP
Weapons Systems Risk Analyst
http://camollc.org
rbeard@camollc.org

Agenda

Problem Statement: Are mitigations effective?

A Step Back

- **Understand problem**
- **Understand role of complex system behavior**

Apply Validated Models: Decomposition

Put Models Together: Connections

Conclusion

Are mitigations effective?

?

Today

Future

Are mitigations effective?

Risk

- Select mitigations
- Select ameliorations
- Select risk transference
- Select risk acceptance
- Commit $ and resources

?

Today

Future

Are the mitigations effective in mission context?

Are mitigations effective?

Risk

Risk against some risk range?

Baseline?

Availability?
Mission Capability?

Today

Risk over a timeframe?

Future

Are mitigations effective?

Approach

Departure

Mission

Takeoff

Landing

Risk

High

4

Medium

Risk against some risk range?

HIGH

4

MEDIUM

Baseline?

Risk against:

- Subjective view?
- Taxi, take-off, departure, en route?
- Mission?
- Return, approach. landing?
- Risk tolerance level?
- A critical system?
- Statement of uncertainty

Risk assumptions:

- Implicit?
- No defense?
- No alternatives?
- Tactical, first-order effect?
- Perfect adversary?

MEDIUM

4

HIGH

Availability?
Mission Capability?

Today

Risk over a timeframe?

Future

Are mitigations effective?

Approach

Departure

Mission

Takeoff

Landing

Risk

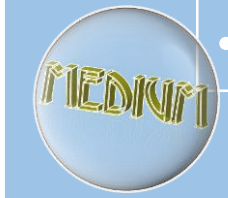
Risk agai

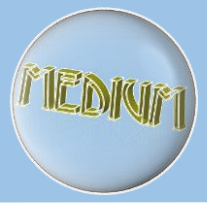
Subjective Claims

Validation of:
- Risk Claim?
- Mitigation Effectiveness?

ssumptions:
plicit?
No defense?
No alternatives?
tical, first-order effect?
t adversary?

Risk tolerance lev
- A critical system?
- Statement of uncertainty





Baseline?

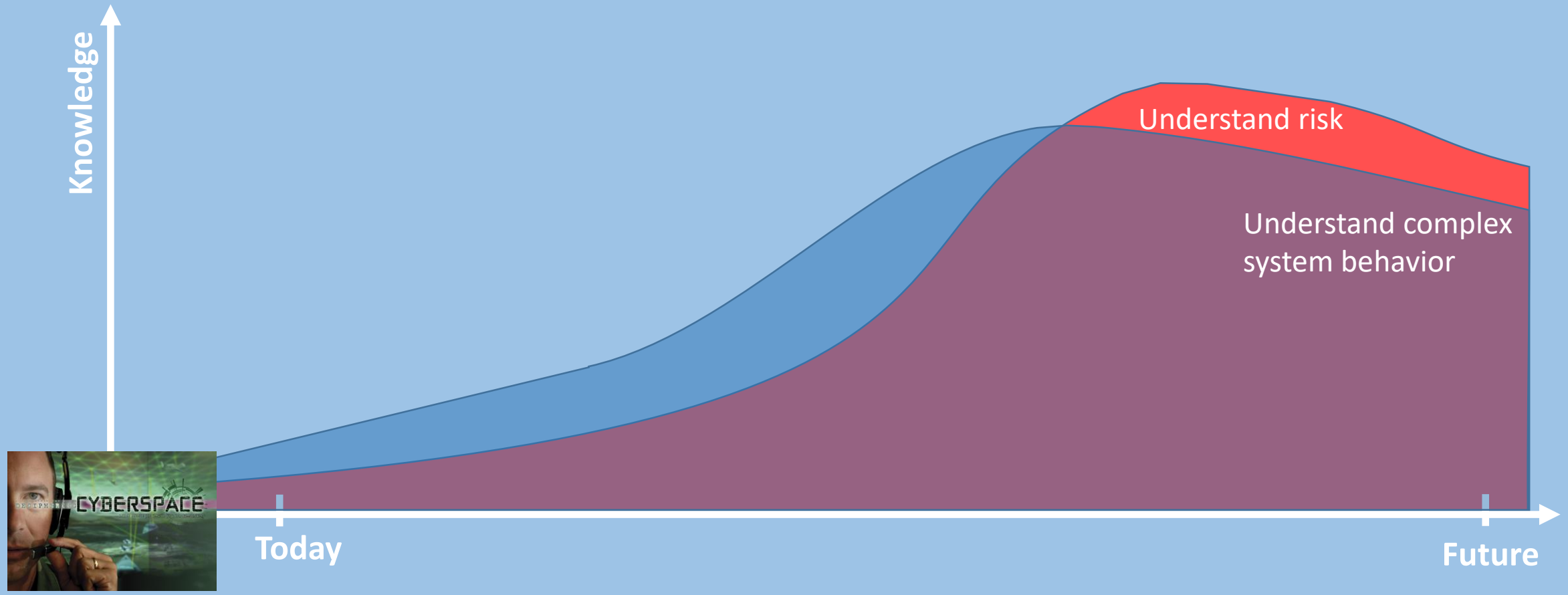
Availability?
Mission Capability?

Today

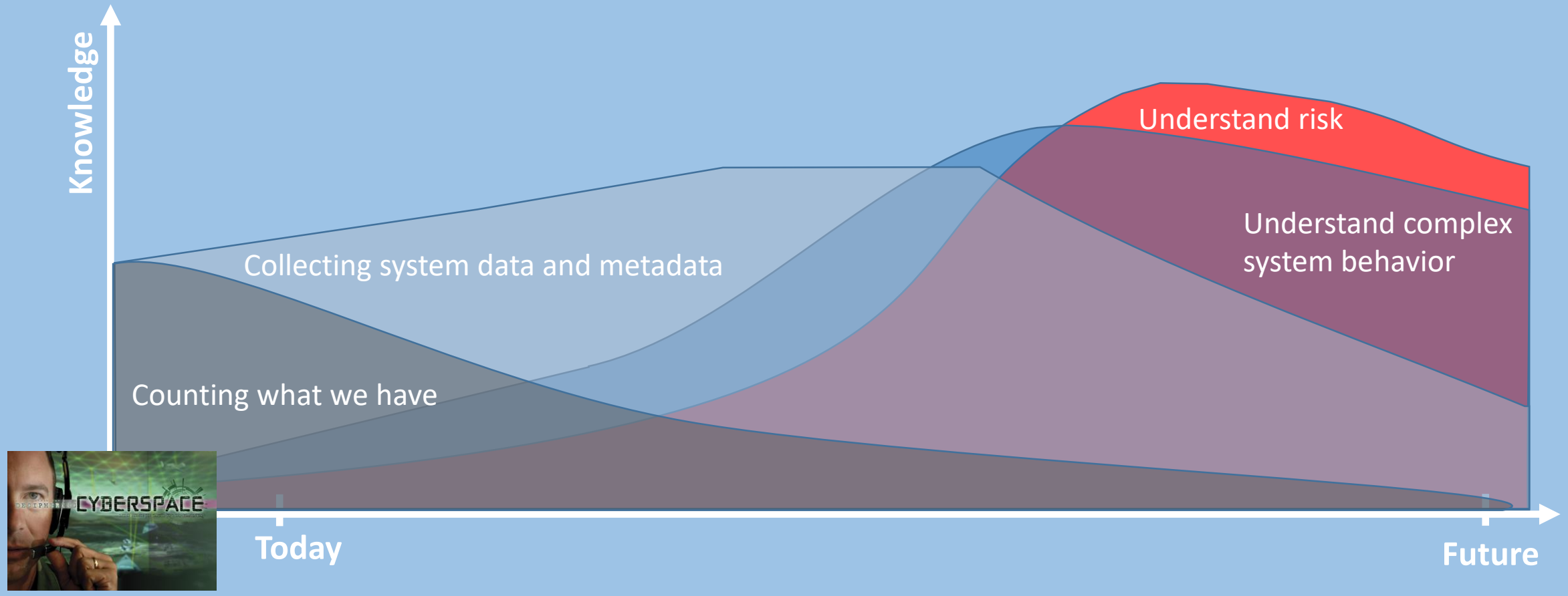
Risk over a timeframe?

Future

A Step Back

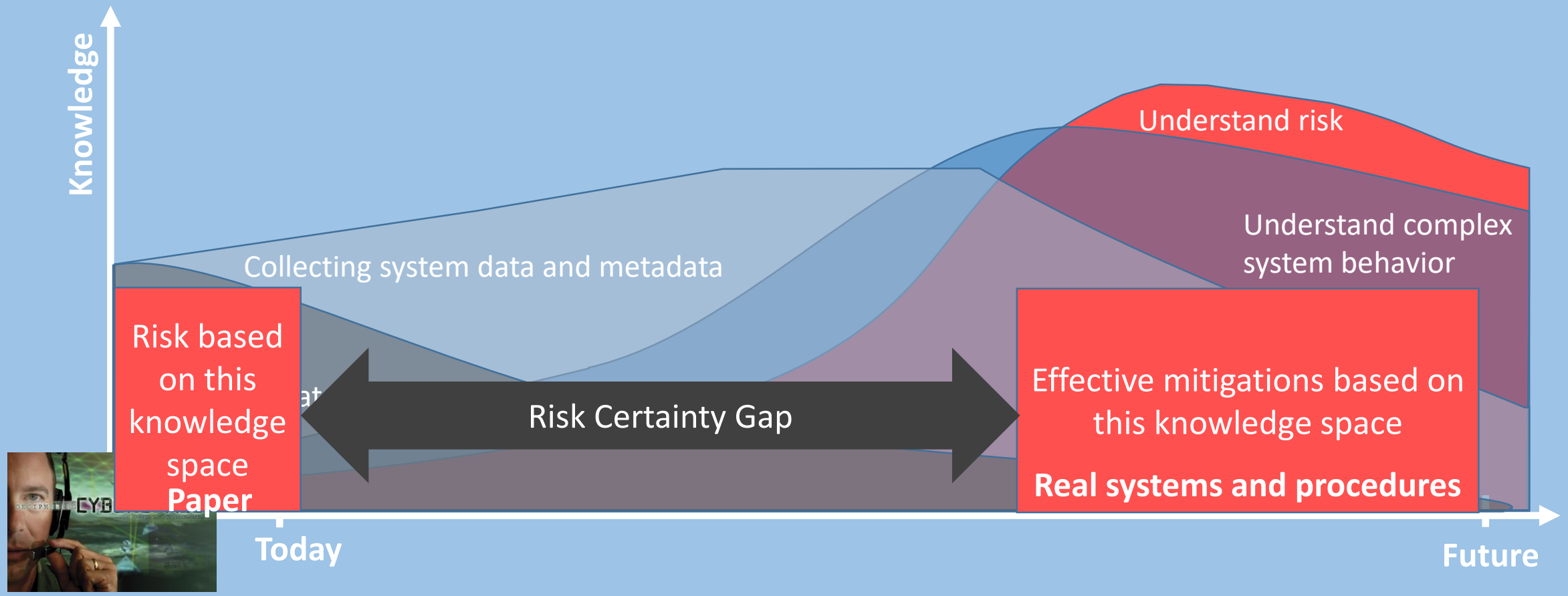

Knowledge
Understand risk
Understand complex system behavior
CYBERSPACE
Today
Future

A Step Back

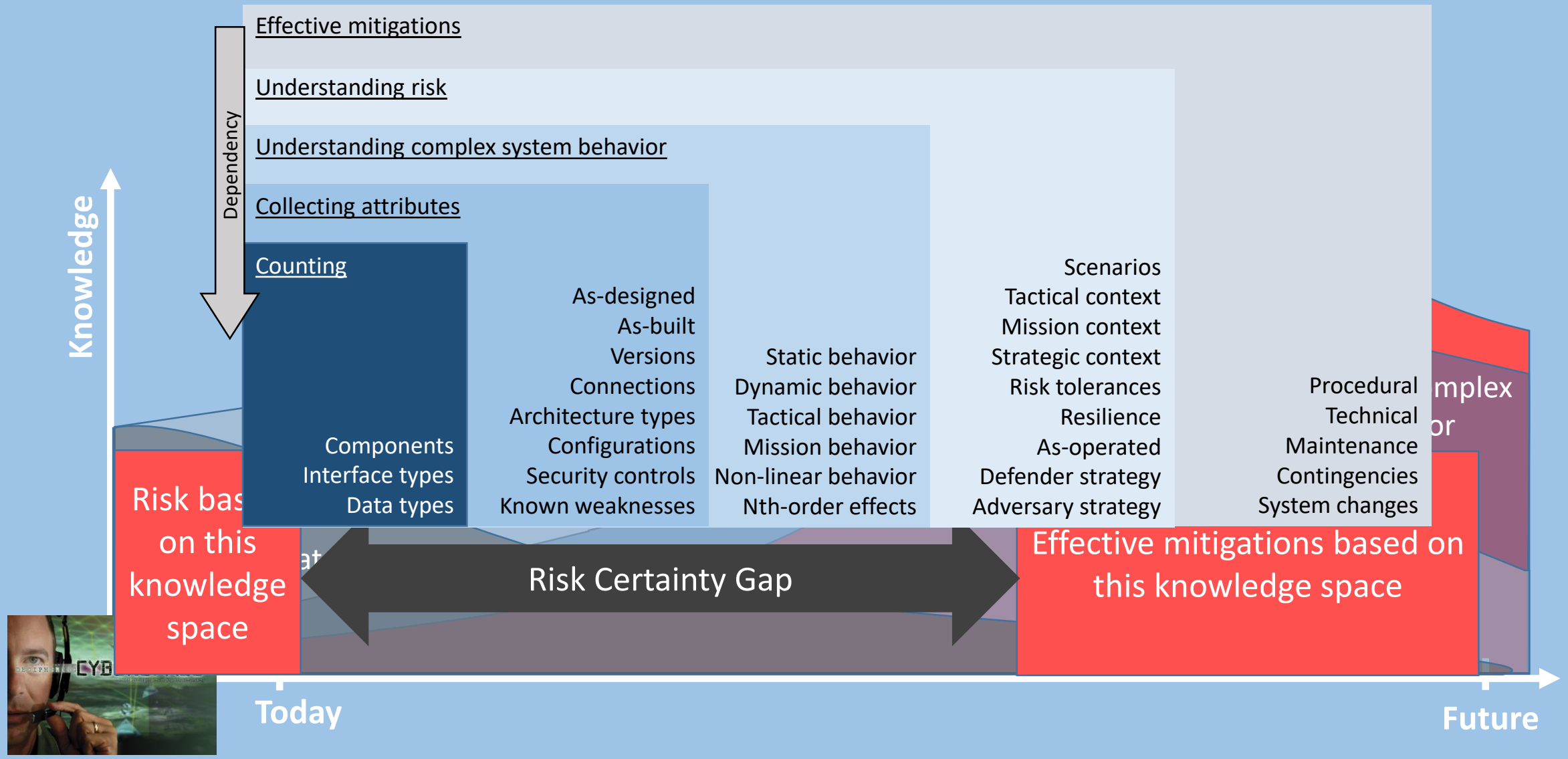

Knowledge
Understand risk
Understand complex system behavior
Collecting system data and metadata
Counting what we have
Today
Future

CYBERSPACE

A Step Back


Knowledge
Understand risk
Understand complex system behavior
Collecting system data and metadata
Risk based on this knowledge space
Paper
Risk Certainty Gap
Effective mitigations based on this knowledge space
Real systems and procedures
Today
Future

A Step Back


Effective mitigations
Understanding risk
Understanding complex system behavior
Collecting attributes
Counting
Dependency
Knowledge
Components
Interface types
Data types
As-designed
As-built
Versions
Connections
Architecture types
Configurations
Security controls
Known weaknesses
Static behavior
Dynamic behavior
Tactical behavior
Mission behavior
Non-linear behavior
Nth-order effects
Scenarios
Tactical context
Mission context
Strategic context
Risk tolerances
Resilience
As-operated
Defender strategy
Adversary strategy
Procedural
Technical
Maintenance
Contingencies
System changes
Risk bas
on this
knowledge
space
Risk Certainty Gap
Effective mitigations based on
this knowledge space
Today
Future

A Step Back

- Test captures new data
- Test validates, refines risk assessment

Analysis and validation cycle

Dependency

Knowledge

Effective mitigations

Understanding risk

Understanding complex system behavior

Collecting attributes

Counting

Components
Interface types
Data types

As-designed
As-built
Versions
Connections
Architecture types
Configurations
Security controls
Known weaknesses

Static behavior
Dynamic behavior
Tactical behavior
Mission behavior
Non-linear behavior
Nth-order effects

Scenarios
Tactical conte
Mission context
Strategic context
Risk tolerances
Resilience
As-operated
Defender strategy
Adversary strategy

Procedural
Technical
Maintenance
Contingencies
System changes

Risk bas
on this

mplex
or

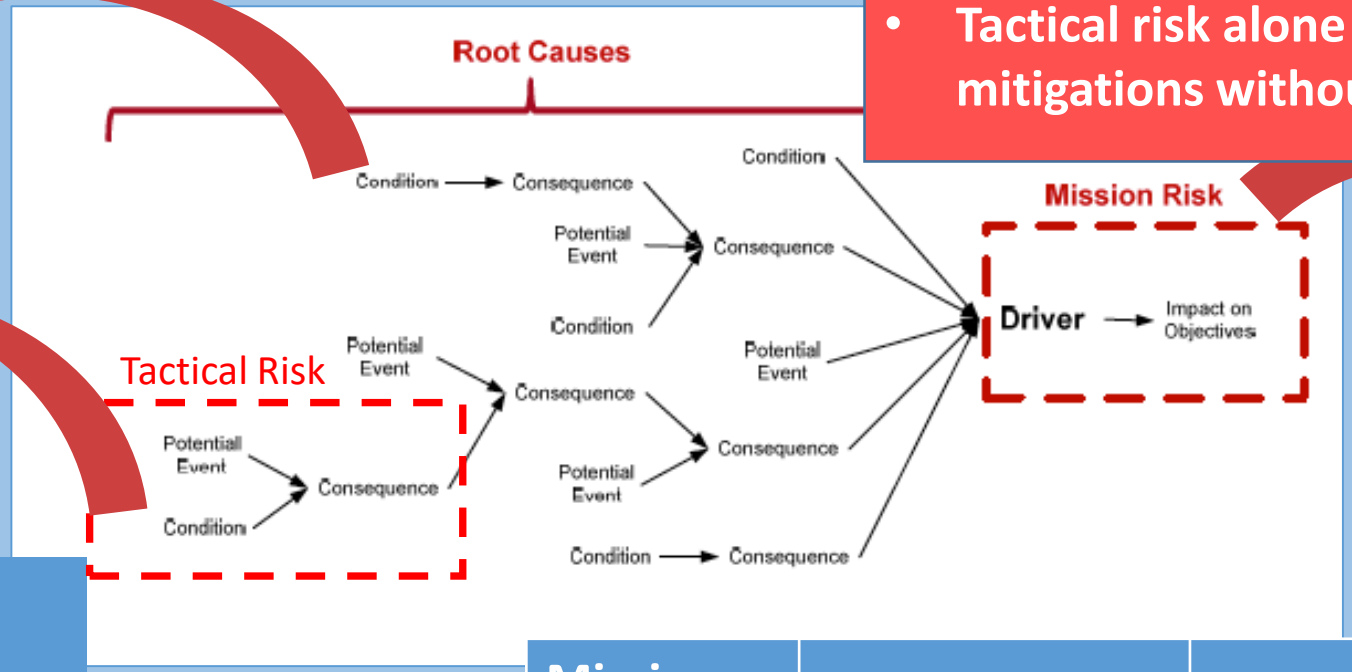
gations based on

Test bridges gap between today and future

- **Understand complex system behavior**
- **Understand risk**
- **Select effective mitigations**

A Mission Risk Model

- Want mission risk
- Tactical risk alone can lead to mitigations without desired effects



Conditions:

- Defender actions
- Adversary actions
- Flight phase
- Operational capabilities
- Mission context
- Situation Awareness

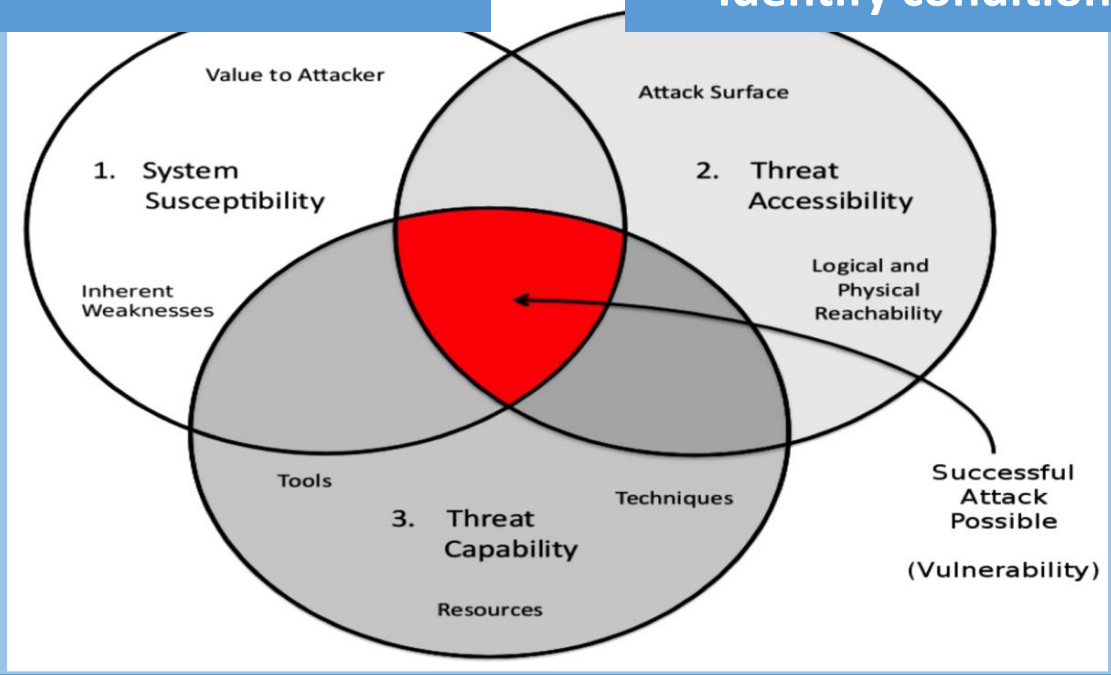
Mission Risk	Confidentiality	Integrity	Availability
Deny			
Degrade			
Deceive			

- Test conditions and capture consequences
- Feed back into risk assessment

A Cyber Threat Model

- Identify new cyber susceptibilities
- Confirm validity of risk assessment susceptibility claims

- Validate risk assessment access point claims
- Identify new cyber threat access points
- Identify conditions for cyber threat access

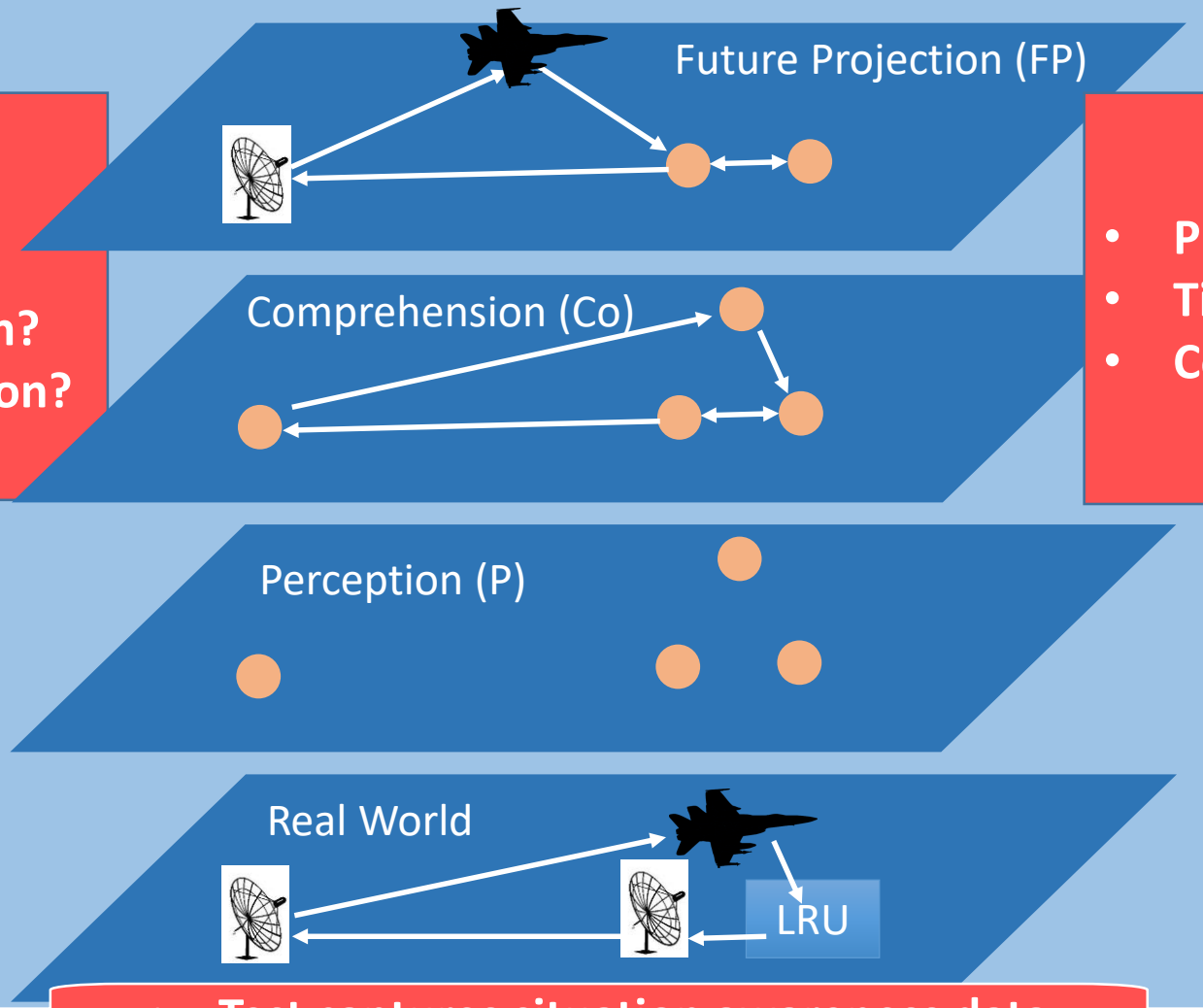


- Capture information about cyber capabilities used to operationally succeed at affecting mission
- Validate or refine risk assessment claims about threat capabilities

- Test captures attributes of cyber threat model
- Feed back into risk assessment

A Situation Awareness Model

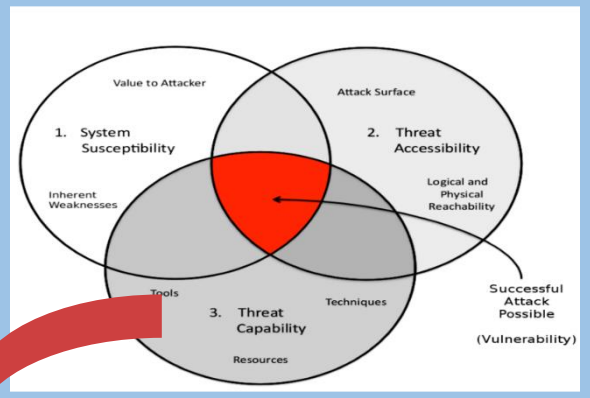
Adversary and Defender
- **Perfect perception?**
- **Perfect comprehension?**
- **Perfect future projection?**

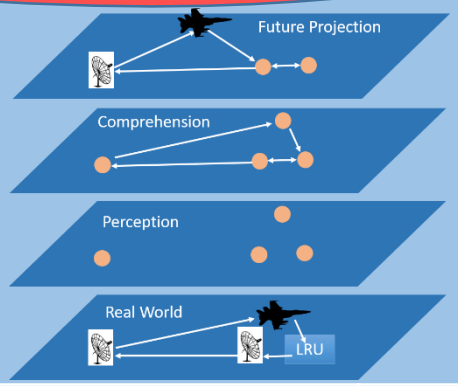


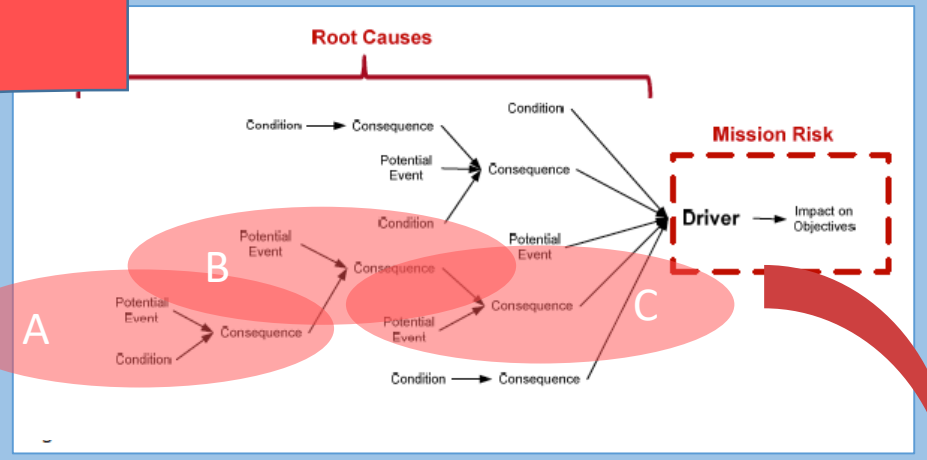
- **Probability**
- **Time to achieve**
- **Cost to achieve**

- **Test captures situation awareness data**
- **Feed back into risk assessment**

Putting it together





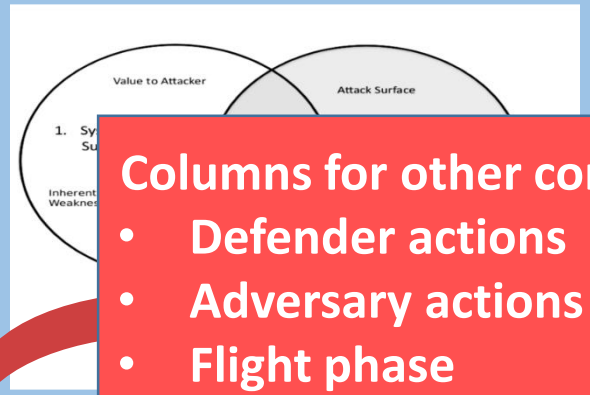


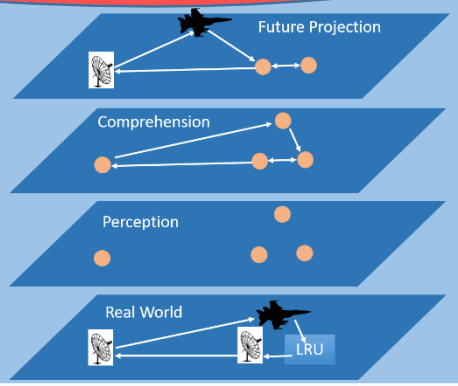
Capability	Conditions: Situation Awareness (Adversary, Defender)			Consequence
	Perceive	Comprehend	Future Projection	
A	• 40% • $1, 1 min.	• 50% • $50K	• 10% • 1 day	
B	• 20% • $100K	• 60% • 1 hour	• 20% • 5 mins	
C	• 70% • $1 M	• 28% • 5 hours	• 2% • 1 week	

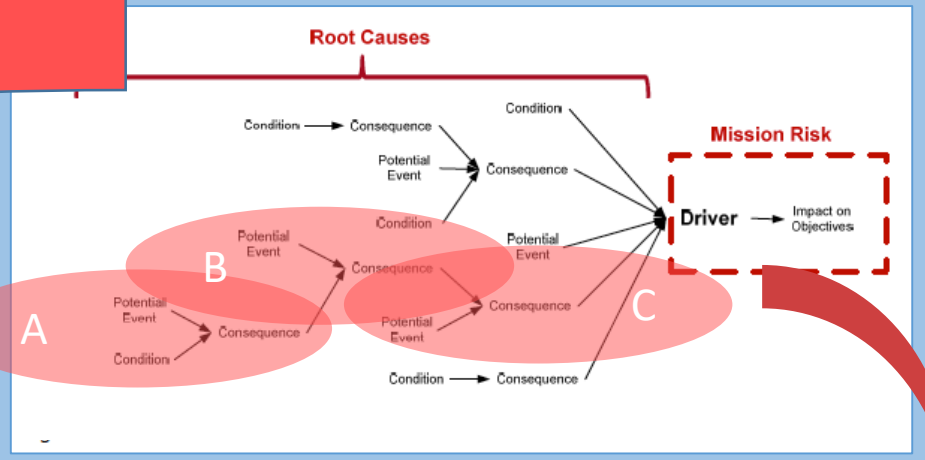
Mission Risk	Confidentiality	Integrity	Availability
Deny			X
Degrade			X
Deceive	X	X	

- Effective Mitigation Targets

Putting it together







Columns for other conditions:

- Defender actions
- Adversary actions
- Flight phase
- Operational capabilities
- Mission context

Table for Access

Cap	ion Awareness Defender)			Consequence			
	Perceive	Comprehend	Future Projection		Mission Risk	Confidentiality	Integrity	Availability
A	• 40% • $1, 1 min.	• 50% • $50K	• 10% • 1 day		Deny			X
					Degrade			X
	• 20%	•					X	
C	• S							

on Targets

- Test captures
- Test validates risk assessment
- Feed test back into risk assessment

Connections create the behavior

Conclusions

Subjective risk assessments leave uncertainty about mitigation effectiveness

We can make more informed mitigation decisions

- Decomposing the problem
- Using validated models
- Understanding complex system behavior

Test can reduce uncertainty

- Quantify complex system behaviors in mission context
- Quantify mitigation effectiveness claims
- Collect data to refine risk assessments
- Collect data to quantify complex system behavior connections
- Grounds risk assessments in reality

Test validates or refines mitigation selection

Questions?

References

- Alberts and Dorofee, *Mission Risk Diagnostic (MRD) Method Description*, Software Engineering Institute, February 2012.
- Cybenko and Hughes, *No Free Lunch in Cyber Security, ACM* MTD ‘14, 3 Nov 2014
- Situation Awareness.
- Cybenko and Hughes, *Three Tenets for Secure Cyber-Physical System Design and Assessment*, Proceedings of SPIE: Cyber Sensing 2014, Jun 2014.
- Endsley, *Toward a Theory of Situation Awareness in Dynamic Systems*, Human Factors, Mar 1995.
- Carin, Cybenko, and Hughes, *Cybersecurity Strategies: The QuERIES Methodology*, IEEE Computer, pp. 20 – 26, 2008.