Smallsat Cyber Security

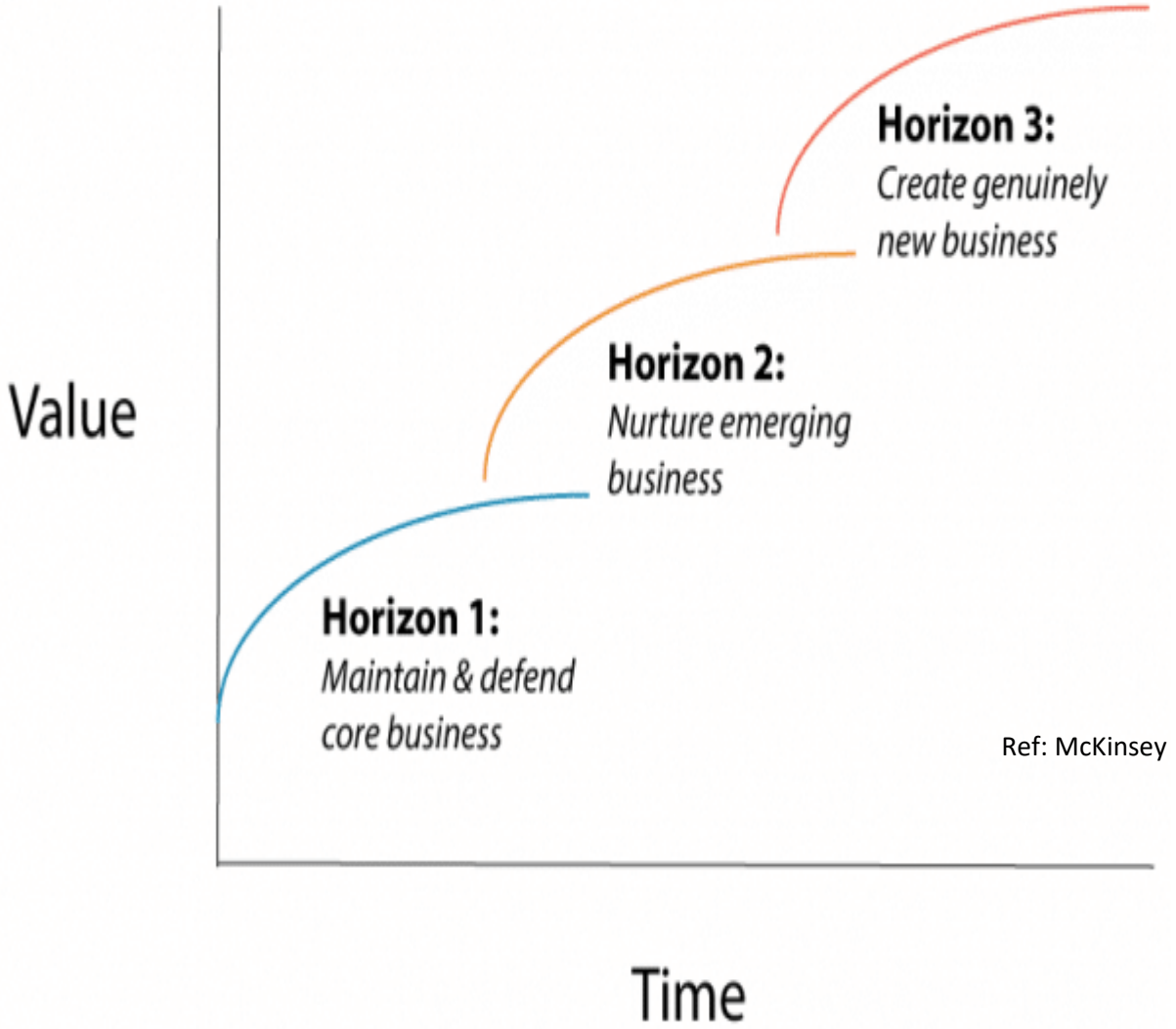
IQM Research Institute
24 Frank Lloyd Wright Drive
Ann Arbor, Michigan 48106

September 25, 2018
Michigan Aerospace Manufactures Association
Space Symposium

IQM Research Institute

- Heritage ERIM model
  - Physics-based Applied R&D Projects
  - Independent 501.C.3
- Innovation Delivery
  - Multi-user Collaboration and Consortiums
  - TRL/MRL 3 through TRL/MRL 7+
- Focus
  - Disruptive Applications (Gaps, Barriers & Pain Points)
  - Reshape Underserved & Emerging Markets
  - Manufactured Products (Commercial and Aerospace)
  - Trusted Position Member
- Locations
  - Ann Arbor, MI (HQ & Labs)
  - Offices -- Washington, DC, Atlanta, GA, Palo Alto, CA

IQM Focuses on Three Horizons of Innovation Value



Ref: McKinsey

2018 State of the Satellite Industry

Global Satellite Industry Revenues

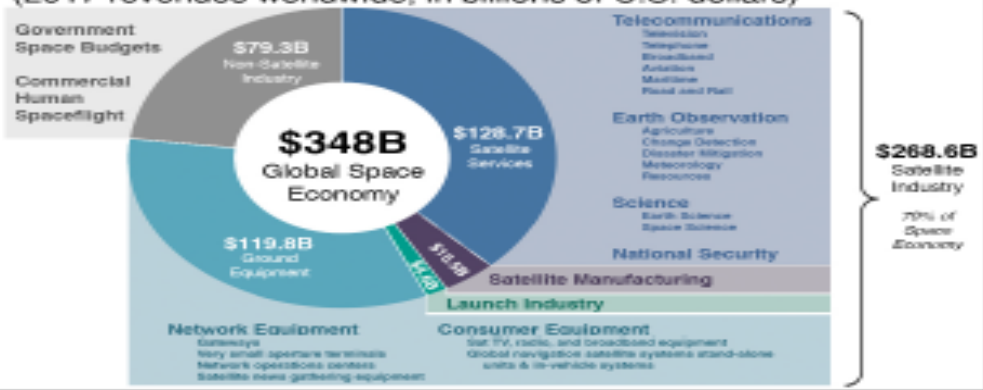
($ Billions)

3%

2016 - 2017 Global Growth

The Satellite Industry in Context

(2017 revenues worldwide, in billions of U.S. dollars)



Satellite Services

1%

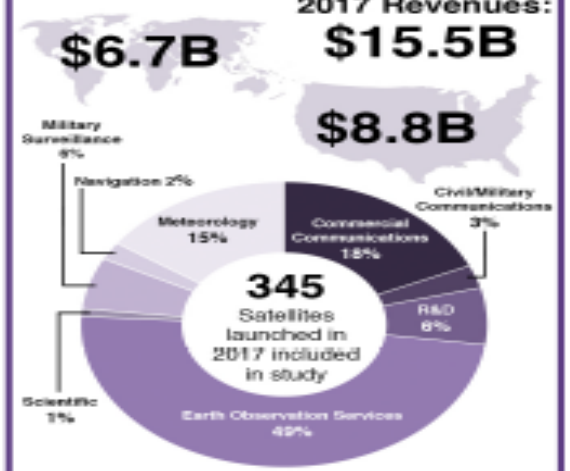
2017 Revenues:
$128.7B

Television	$97B
Radio	$5.4B
Broadband	$2.1B
Fixed	$17.9B
Mobile	$4B
Earth Observation	$2.2B

Satellite Manufacturing

10%

2017 Revenues:
$15.5B

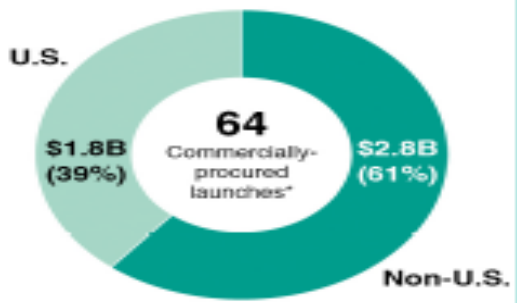


Satellites Launched by Mission Type

Launch Industry

16%

2017 Revenues **$4.6B**



** There were 90 total orbital launches in 2017. Of these, 64 were commercially procured, 13 were not commercially procured, and 13 involved space vehicles.*

Commercial Launch Revenues by Region

Ground Equipment

5.6%

2017 Revenues **$119.8B**

$108B
Consumer Equipment
(GNSS devices/chipsets, satellite TV dishes, etc.)

GPS

$11.8B
Network Equipment
(VSATs, gateways, etc.)

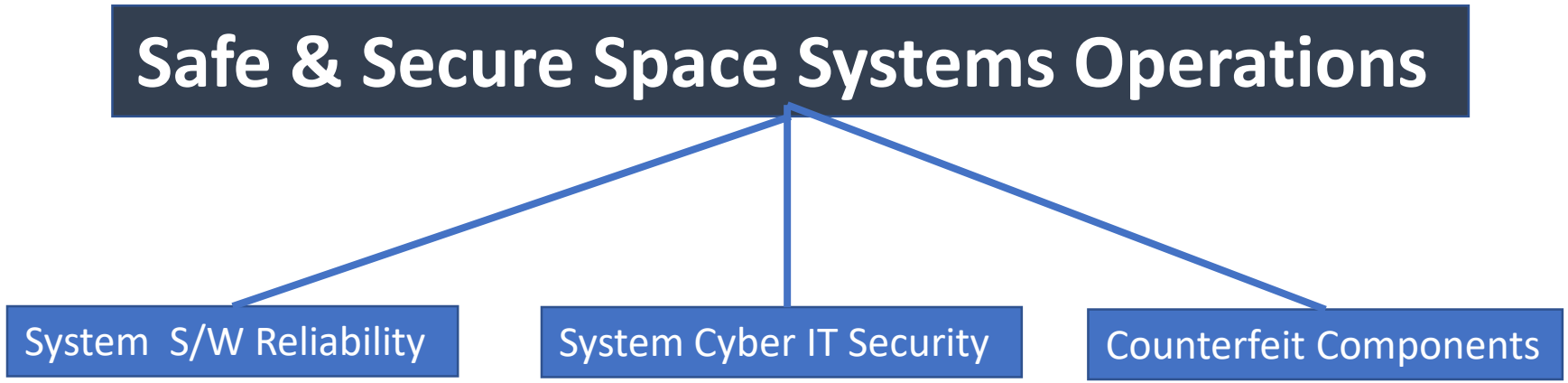
BRYCE

Produced by Bryce Space and Technology (formerly Tauri Group Space and Technology)

Focus Areas of Space System Cybersecurity

- Mission Payload System
  - Subsystems
  - Integrated
- Mission Support Systems
  - Checkout & Launch
  - Satellite Control
  - Data Link
- Enterprise Support Systems
  - 3rd Party Providers

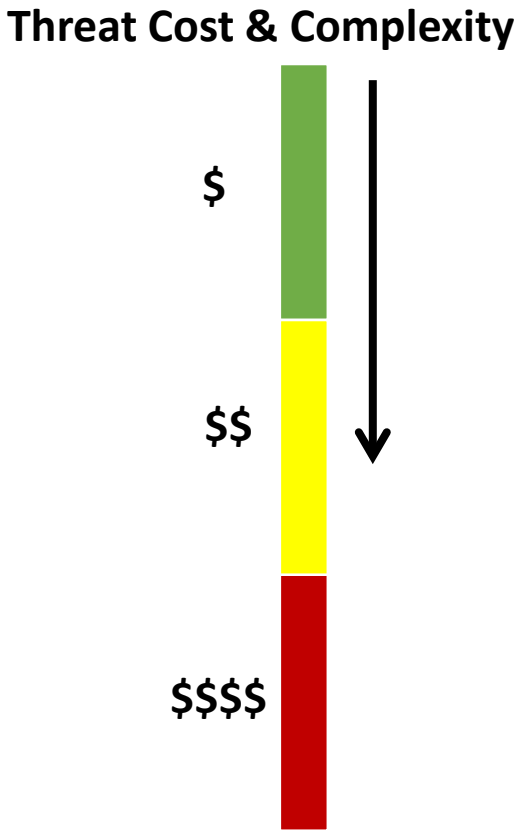
Framing the Issues



Reliability, Cyber Security, & Trusted Components

Smallsat/Cubesat Cyber Threat Construct

- Level I – Hacker Threat
  - Close Hacker Pathways
- Level II – Unknown/Unknown Threat
  - Evolve new Architectures and Subsystems
  - Protect design, manufacture, infrastructure
- Level III – Nation State Attack
  - Outside Industry R&D Purview
  - Partnership with DoD Organizations



Gap Exists Between Current State of Practice and the Escalating Creativity of Threat Actors

Cyber Policy for DoD Space Systems

- **Presidential Policy Directive (PPD-4)** "National Space Policy of the United States of America"
- **Committee on National Security Systems (CNSS) Series** "National Information Assurance Policy for Space Systems Used to Support National Security Space Systems"
  - CNSSD 505 – Supply Chain Risk Management
  - CNSSI 1200 – Risk Management Framework
- **DoD CIO**
  - DCIO 8581-01- Information Assurance Policy for Space Systems Used by the DoD (new Memo in 2019)
  - Encryption to and from platform & payload generated data
- **CNSS Secretariat** – Responsible for tracking Member and Observer Organizations
- **USSTRATCOM** – Responsible for Enforcing Across Multiple DoD Agencies
- **AFSPC/SMC** – Implementation in Acquisition Programs
  - Contract Terms and Conditions

IQM

Advancing technology for the betterment of mankind

Commercial Space Standards & Practices for Cyber Security

- **Presidential Policy Directive (PPD-4)** – *Focus on Intent*
- **National Space Council & Federal Aviation Agency Activities** – *Focus on Space Traffic Management & Space Debris Prevention*
- **Pure Commercial Smallsats/Cubesats Systems**
  - Open Source Architectures & Components
  - Applicable NIST Standards (NIST 800 Series)
  - Security Information & Event Managers/SCAP Validated Products
- **Gray Area – National Defense Authorization Acts (2016/2017/2018) Defense Industrial Base**
- **Standards Organizations**
  - IEEE
  - SAE
  - CEN/CENELEC

Smallsat Cyber Workforce Education Issues

Severe Shortages within Cybersecurity Workforce

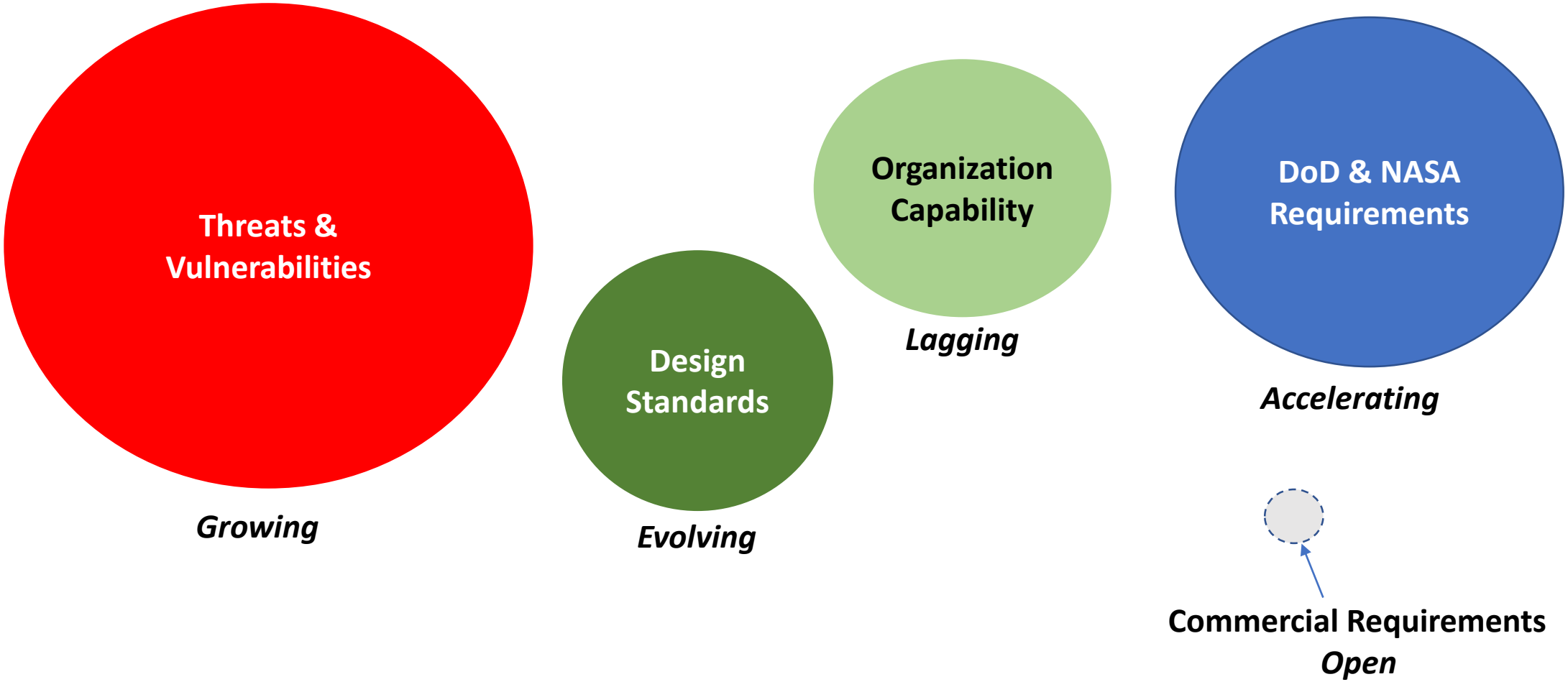
University & College Education Limitations

Curriculum Planning & Content

Laboratory Equipment

Student Grand Challenges

Where are We Today?



The Smallsat/Cubesat Cyber Future

- **Smallsat Cyber Security is not a "One and Done" Issue**
  - *Growing Market Continues to Attract Evolving Threat Actors*
- **Unacceptable Current Status Quo Against Evolving Threats**
  - *State of Practice - Bimodal Mix of Secured & Unsecured Designs*
- **Leaning Forward in Mission Assurance**
  - *Increased Use of Encryption*
  - *Emerging Policies, Better Design Standards & Best Practices*
- **Structural Weaknesses**
  - *Poor Cyber Hygiene in Enterprise Systems*
  - *Lack of Wide Scale Engagement of Federal-sponsored Cyber Resources*
  - *Component and System Level Compliance Testing*
  - *Workforce*