PORTFOLIO ARCHITECT

Resilient Space Services Through Hybrid Military/Commercial Architectures

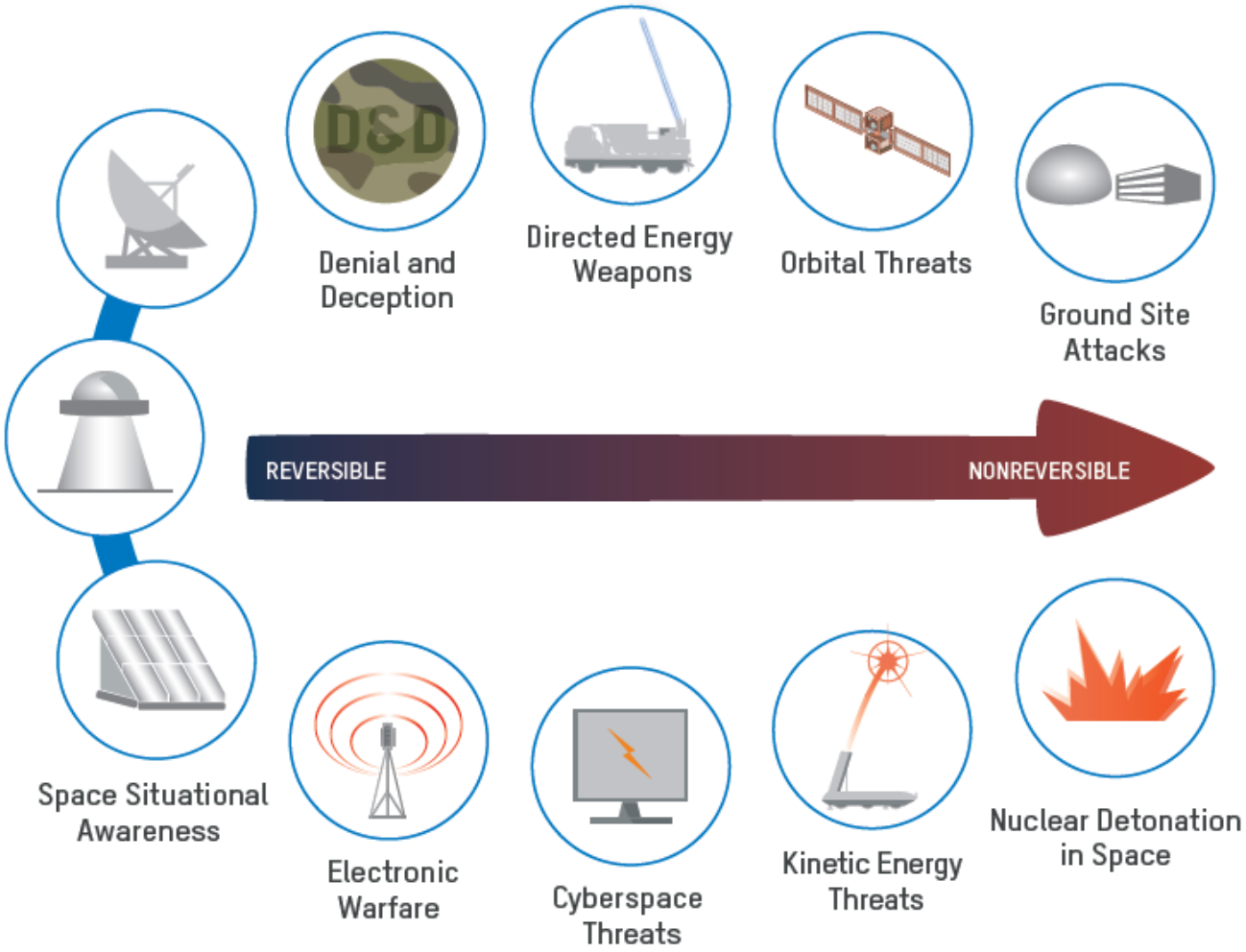
4 March 2020

Clay Bosler

LinQuest Corporation

© 2020 by LinQuest Corporation. Published by The Aerospace Corporation with permission

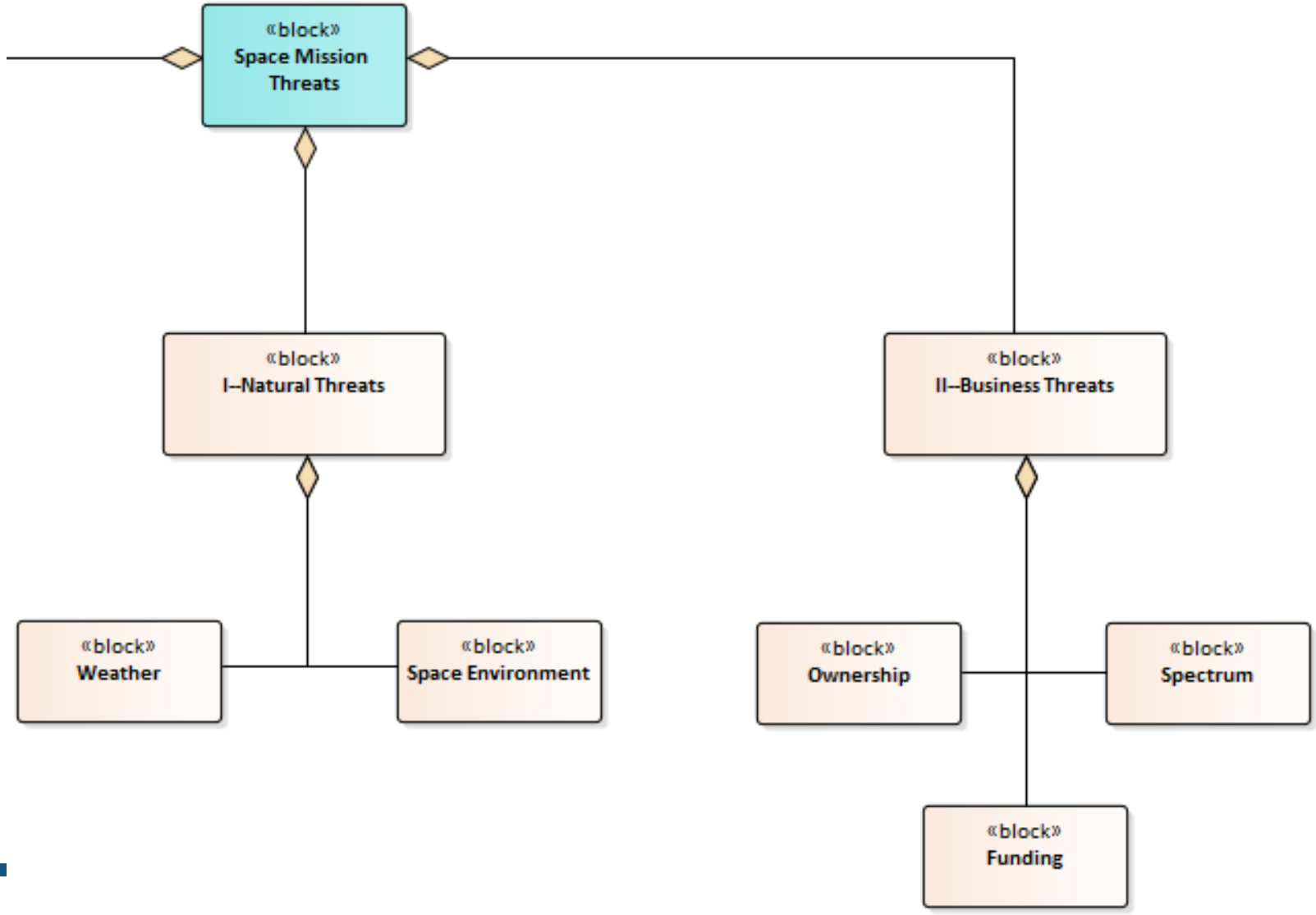
Counterspace Threat Continuum…



Visualization: DIA, D3 Design • 1811-20013

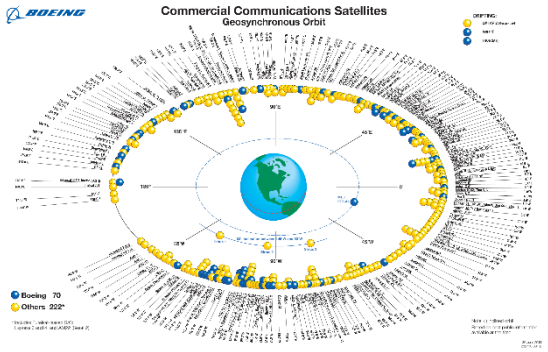
1

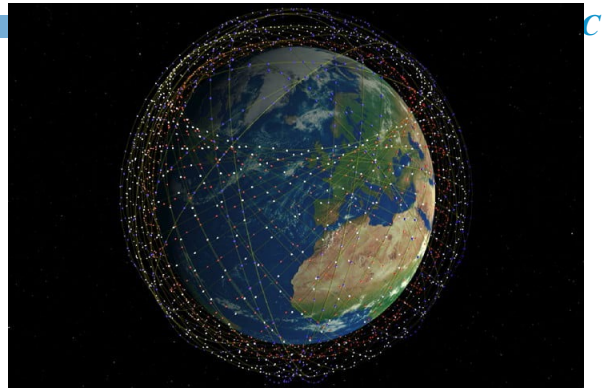
… and Some Other Threats



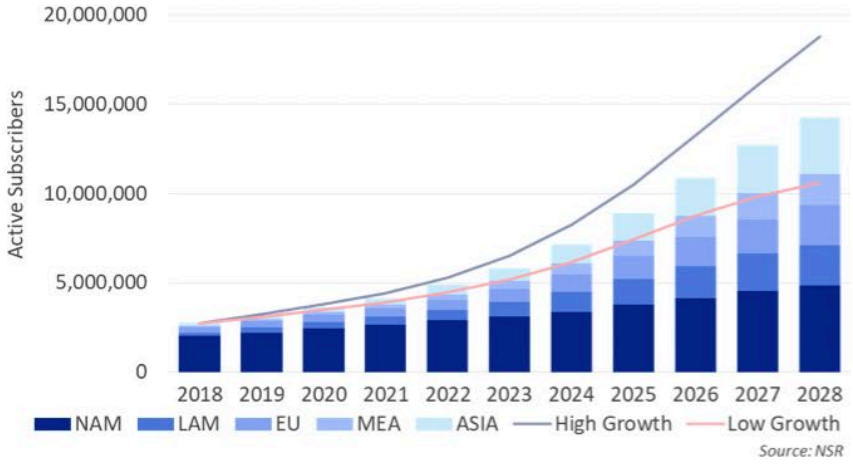
2

“New Space” offerings





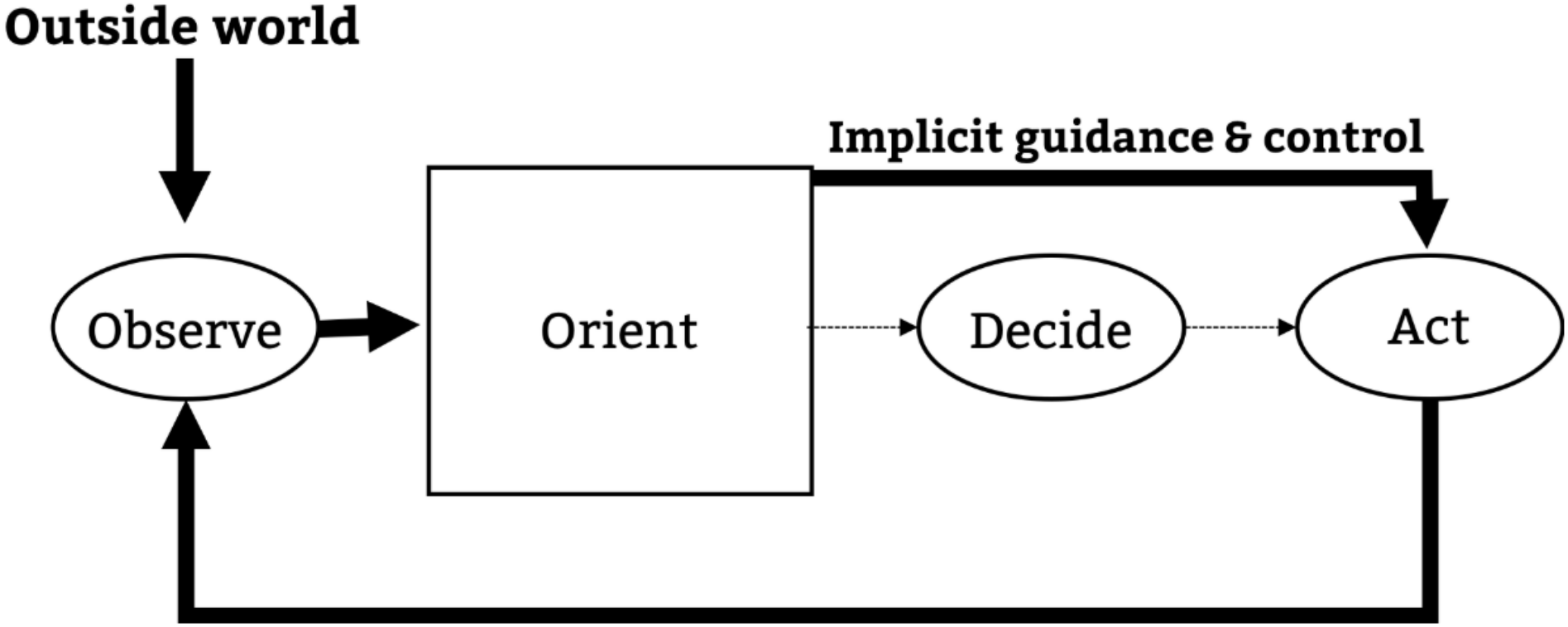
Consumer Broadband Subscribers by Region



Enterprise VSAT Capacity Revenues

“New Space” services outstripping traditional and military capabilities

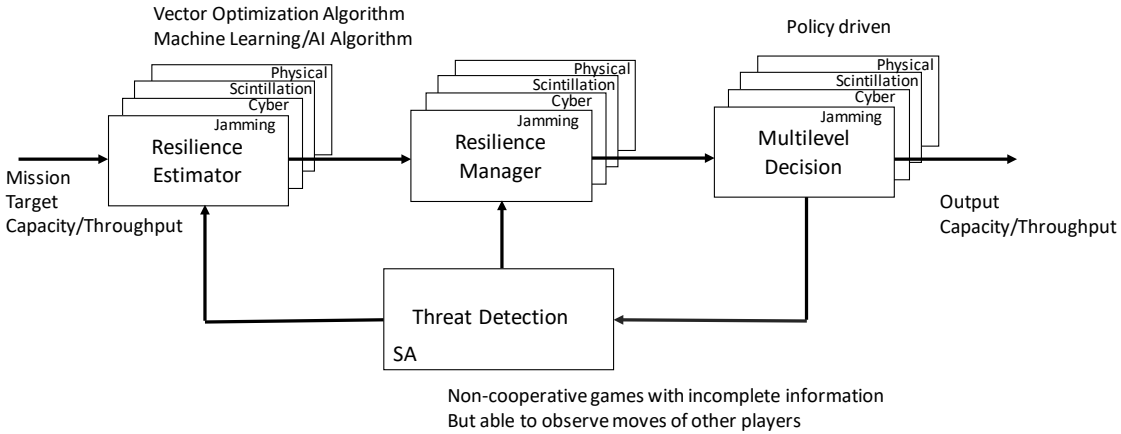
Trust and Culture



4

Trust and Culture – A Resilience Control Loop

PORTFOLIO ARCHITECT



- **Input: A scenario or a mission with a target capacity/throughput**
- **Output: Delivered capacity/throughput in the presence of attacks**

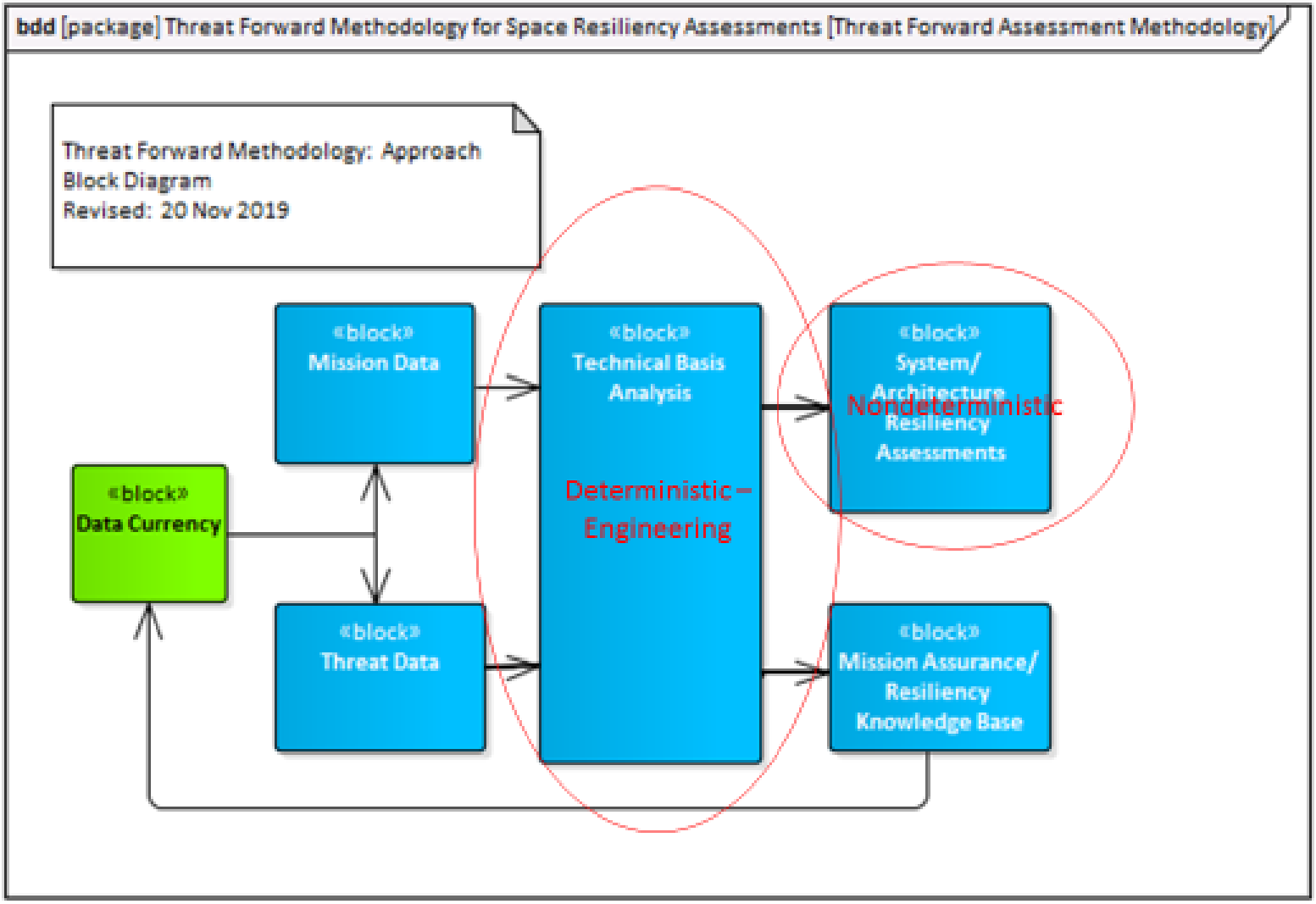
- **Control loop operates across domains with each domain having different cost and payoff over the duration of interest**
- **Control loop timelines extend from milliseconds to decades**
  - Robust
  - Not too sensitive (bang-bang)

5
5

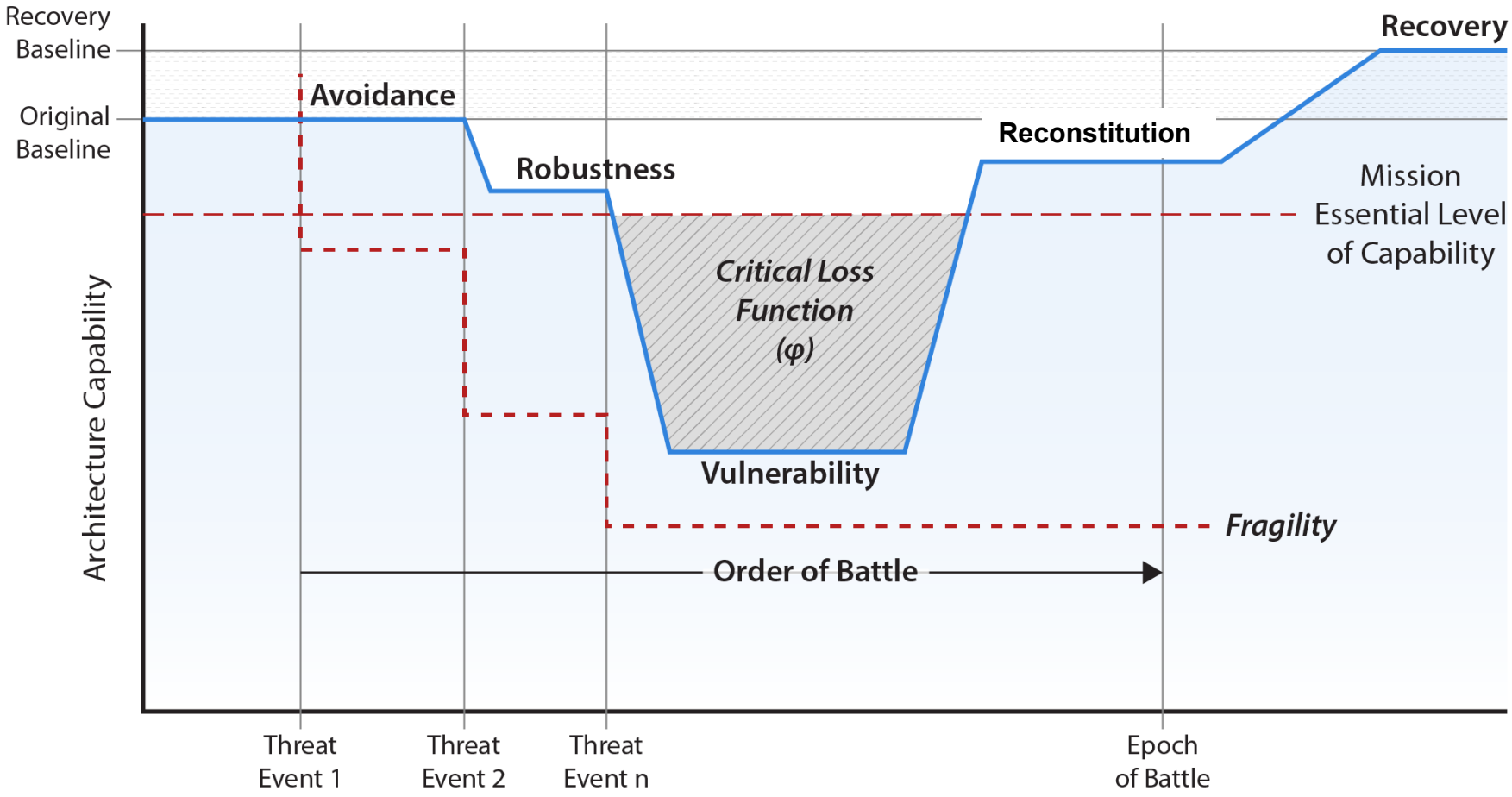
Some control loop considerations

- Traffic priority
  - CJCSI 6250 (static)
  - Next generation - dynamic
  - 5G
- Levels of Hostility
  - Business, Weather, Space Weather
  - Cyber
  - Jamming
  - Kinetic (Space and Terrestrial)
  - Nuclear Scintillation
- Traffic Type
  - VOIP
  - Video
  - Data, etc
- Routing preferences
  - Business considerations
  - Routing considerations
- Adversarial considerations
  - Game Theory
  - Agent Based Modelling
  - Linear Programming

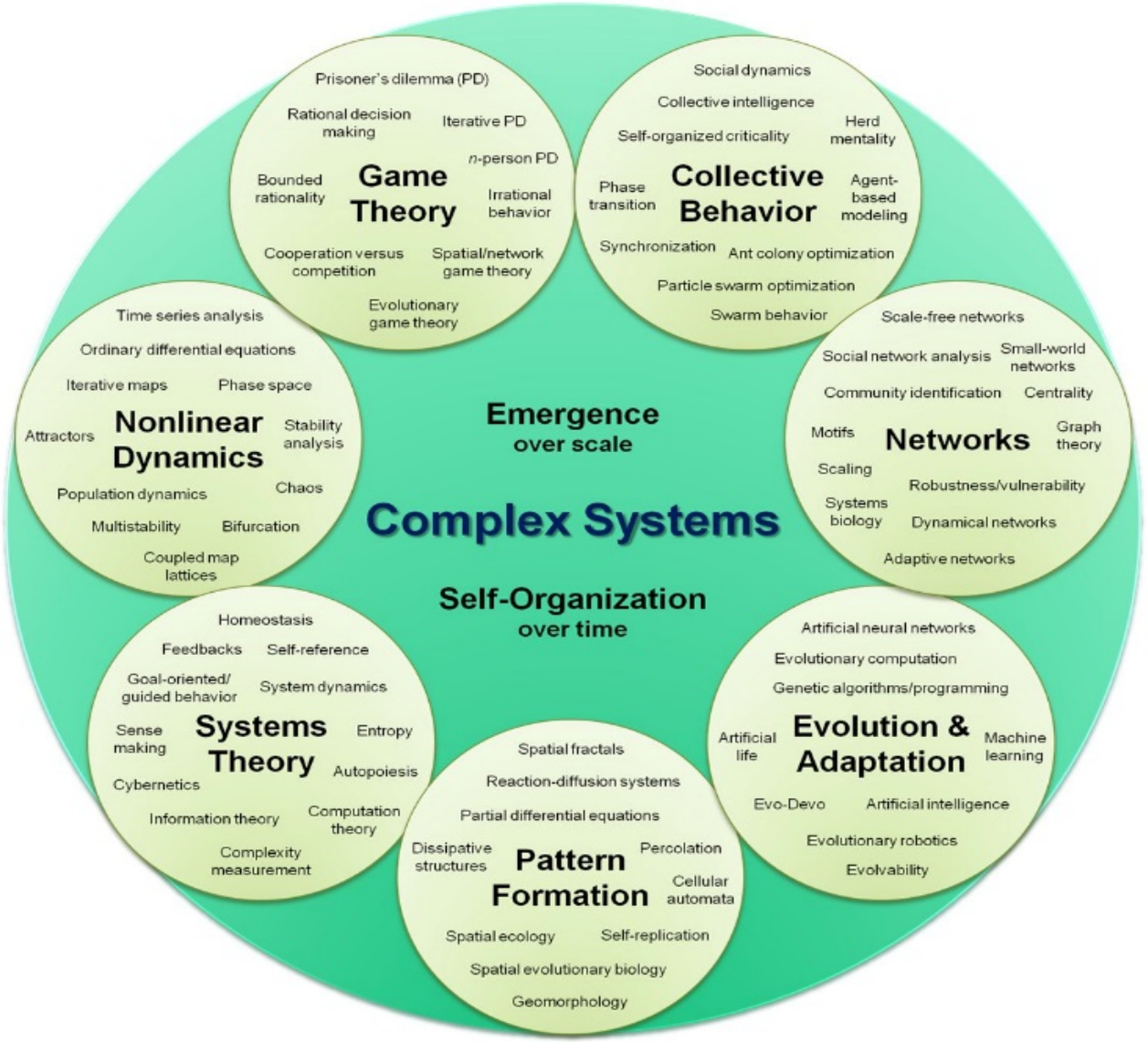
Tying it all together – Threat Forward!



Threat/Response Timeline



Moving into complexity science…



PORTFOLIO ARCHITECT

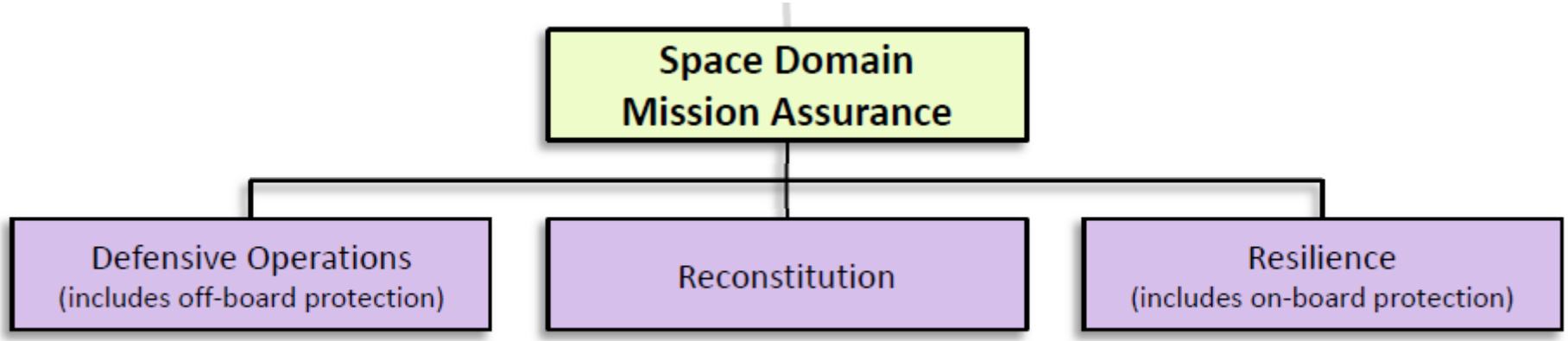
Backup Slides

Space Policy (DoDD 3100.10)

- Required level of space mission assurance is based on the type of operation supported and must be consistent with the Assured Space Operations Framework:
  - *Tier 1. Endurable, survivable, and continuously available through all phases of conflict and levels of hostility.*
  - *Tier 2. Present through all phases and levels of conflict with possible quality or quantity limitations and transient or localized outages; capable of reconstitution on tactical timelines.*
  - *Tier 3. Restorable based on rear echelon and homeland security needs; could be lost during highest levels of conflict.*

11

Space Domain Mission Assurance Taxonomy

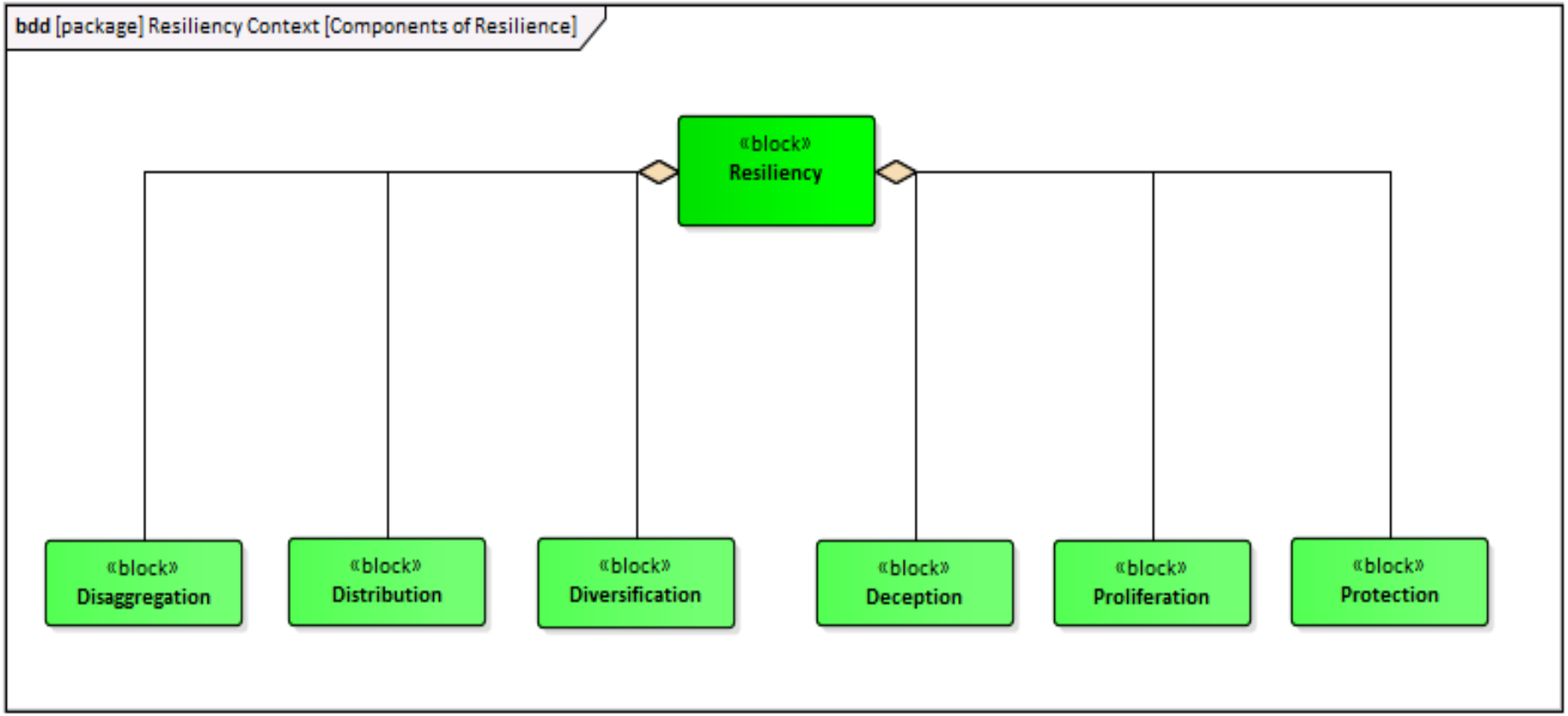
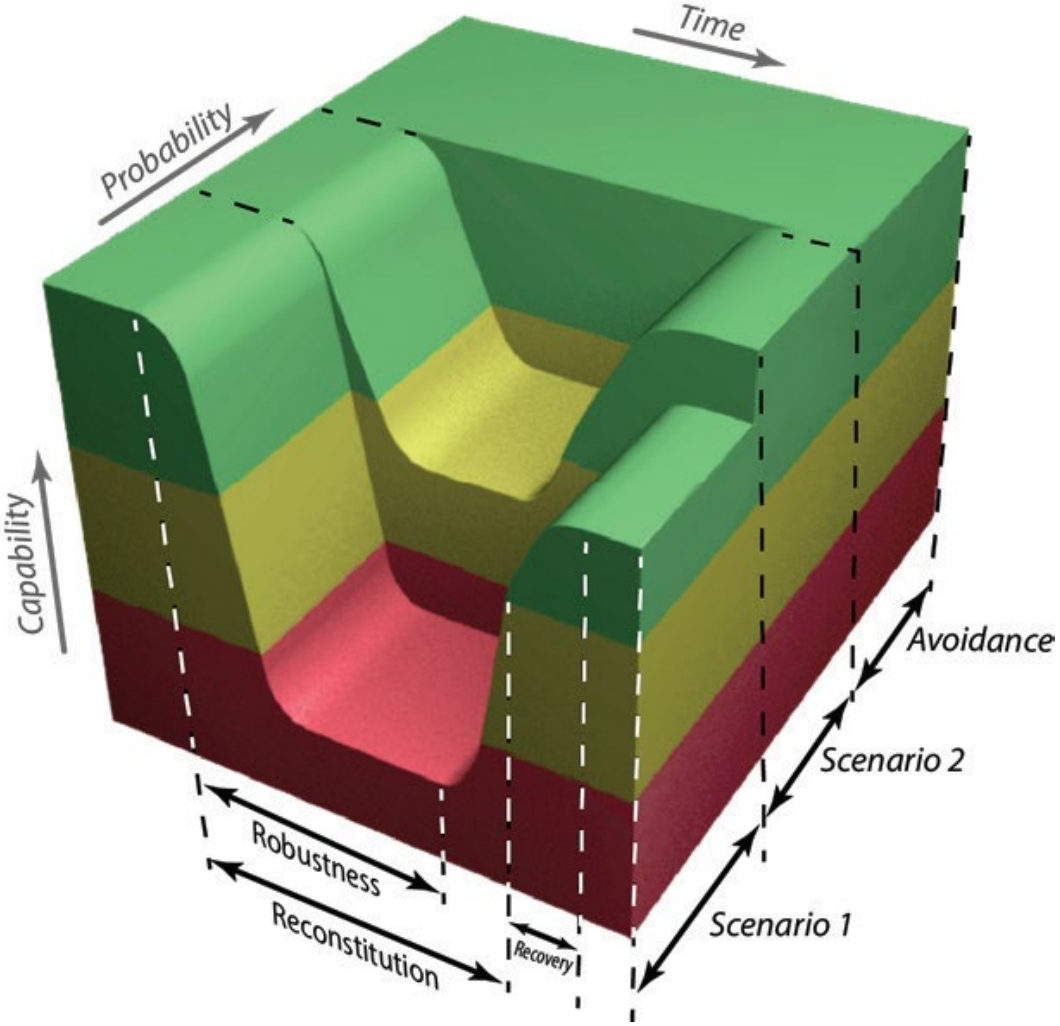


Defensive Operations: *Activities or operations undertaken to interrupt an adversary kill chain, or provide warning or insight to the targeted mission system in support of defensive actions.*

Reconstitution: *Plans or operations to bring new assets on line (e.g. launching replacement satellites or activating new ground stations) in order to replenish lost or diminished functions to an acceptable level for a particular mission, operation, or contingency after an attack or catastrophic event.*

Resilience: *The ability of an architecture to support the functions necessary for mission success with higher probability, shorter periods of reduced capability, and across a wider range of scenarios, conditions, and threats, in spite of hostile action or adverse conditions*

Space Domain Mission Assurance Taxonomy - Resiliency



Threat/Response Timeline