

Cyber Mission Impact Assessment and Response

Scott Musman

703-983-2379 • smusman@mitre.org

Aaron Temin

703-983-7330 • atemin@mitre.org

AF MOIE



The Problem



“We are not defending our networks, we’re defending our operations”

LTC VanPutte, PM DARPA, while at JTF/GNO

- **Current security systems report only the activity they detect**
 - They do not identify mission relevance or estimate mission impact.
- **Hence, the importance of components is often over stated**
 - Data, Users, Systems become labeled as critical ALL the time.
- **When a cyber incident occurs we don’t know what impact it will have on our mission(s)**
 - Which mission elements are affected? Can we continue to operate and fulfill the mission? Can we reconfigure? Can we salvage “part” of the mission? Which are the right parts to salvage?

- **Mission Assurance must leverage knowledge of the mission and what is important, to which mission elements, when**
 - There needs to be a mission model

Background



- **Our adversaries have declared that they intend to deny us use of our networks should we enter a conflict**
 - They are investing heavily in asymmetrical capabilities.

- **We presume that our enemies are already inside our networks:**
 - Will we be able to successfully operate in the face of their activity?

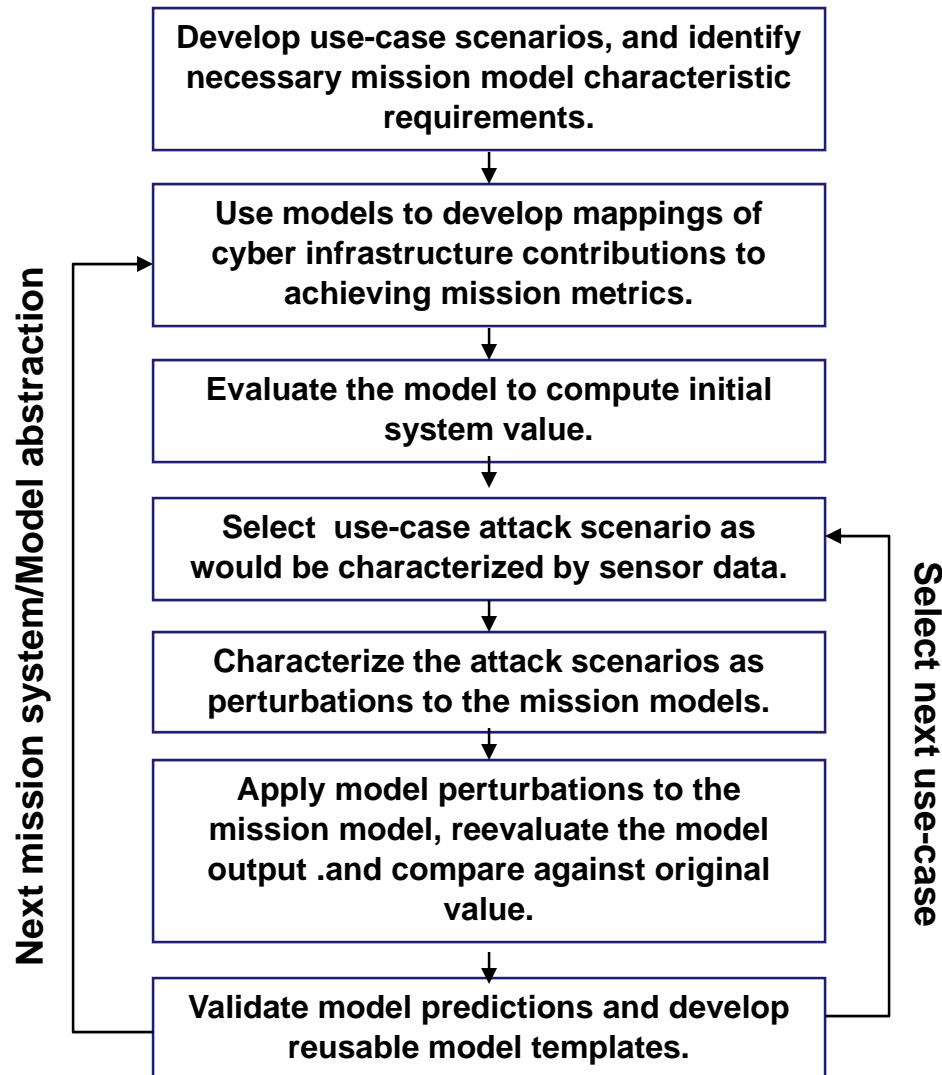
- **We need techniques that help us to effectively comprehend and then respond to cyber incidents.**

Objective



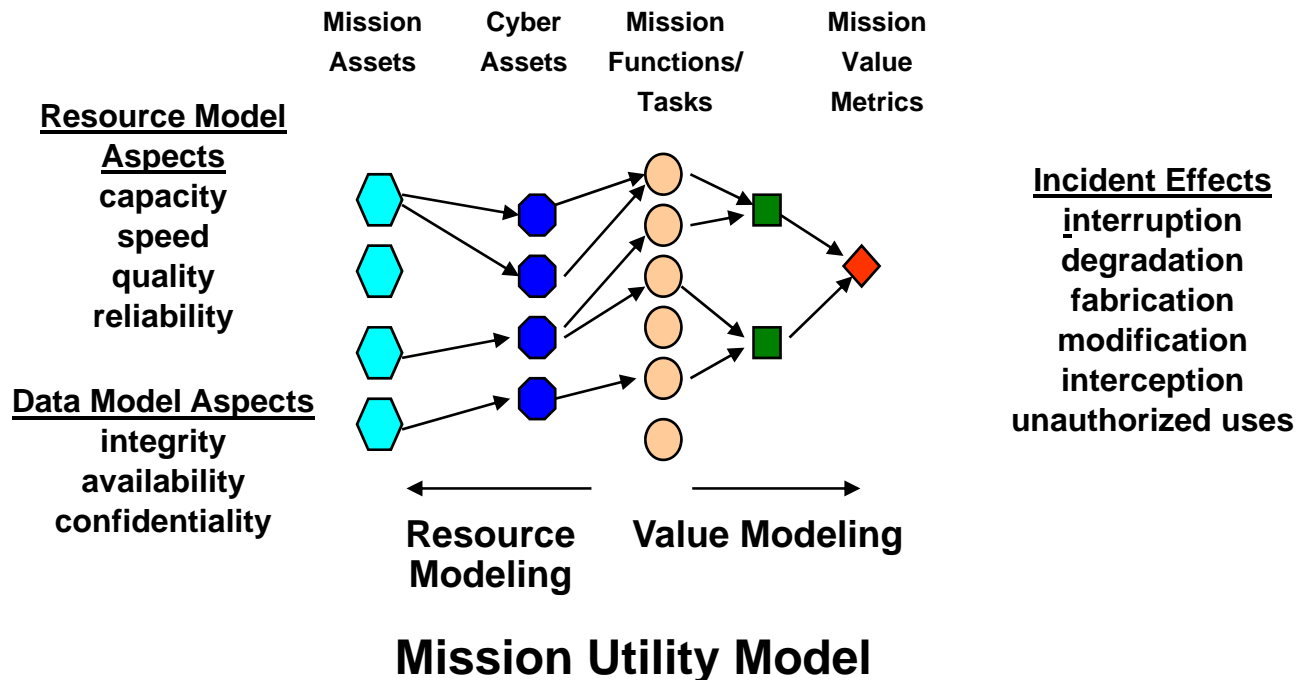
- **Explicitly capture in computable form details of missions, system characteristics, and cyber incidents**
 - Avoid “implicit” encoding of knowledge/relationships.
- **Map the relationships between mission functions, mission assets, cyber assets, and mission related value metrics**
 - Not just the dependencies, but we also include the timing information.
- **Develop techniques to compute Mission Impact of Cyber Events**
 - We expect to also be able to use this to assess response actions that would mitigate/minimize mission impact.
- **Demonstrate the value of our techniques using before/after and with/without comparisons**
 - Different modeling choices, a variety of use-cases.
- **Generalize the results across multiple mission systems**
 - Understand the implications of modeling detail
 - Comprehend generality of mission models and modeling elements.
- **GOAL: Develop a working prototype and supporting tools that can make this widely practical**
 - Applied to several sponsor missions.

Activities

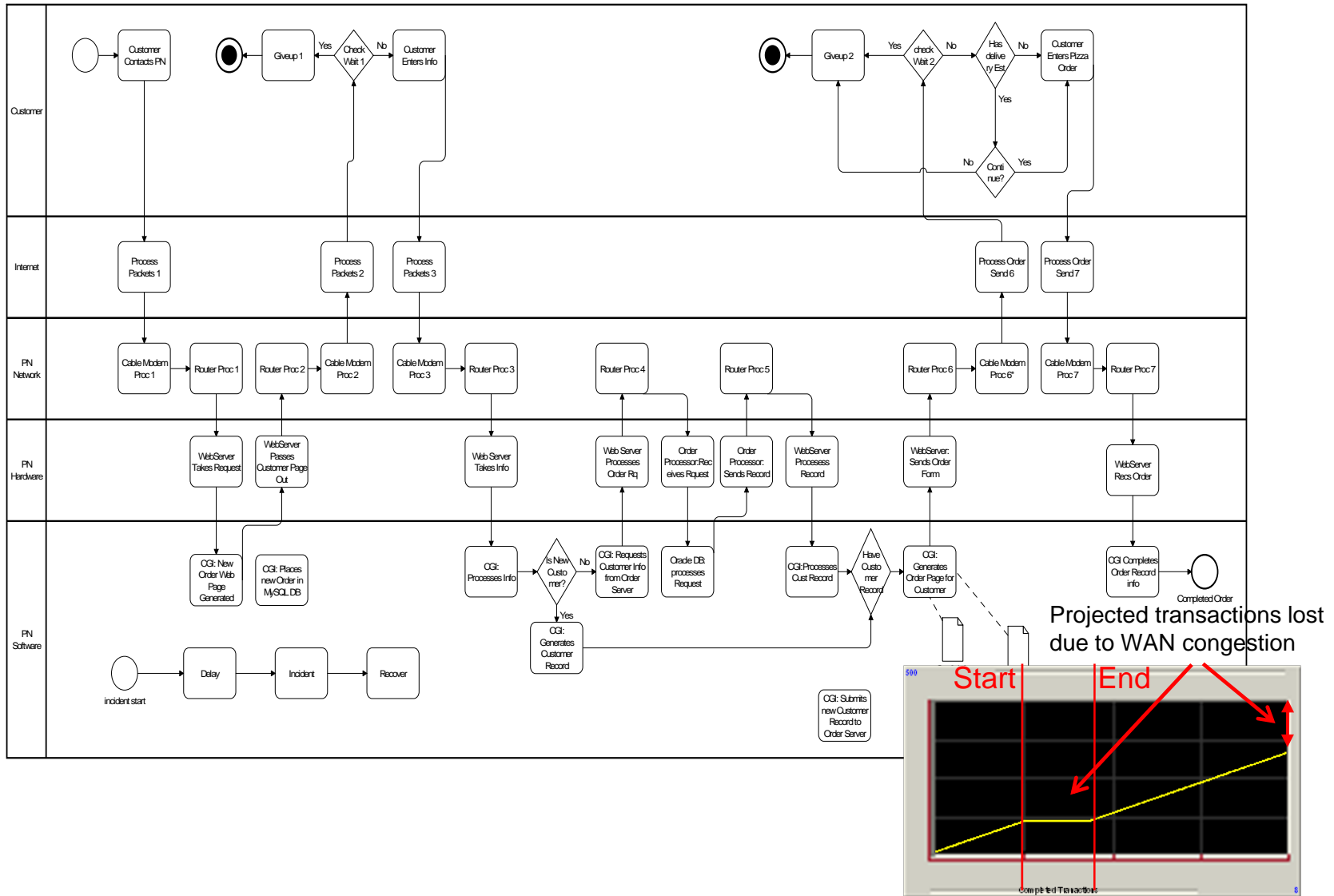


Highlight

- Task oriented models include resource dependencies and value relationships
 - Influence diagrams are the core technology we will use.
- We model the intrinsic characteristics of cyber components that make them suitable to perform mission activities
 - We anticipate model reuse across similar cyber components.



Demonstration



Impacts



- **Provide timely estimates of the “mission impact”**
 - How can you do mission assurance without a model of the “mission” and how the cyber infrastructure supports it?
- **Improved Cyber SA**
 - Not just the events and systems, but the mission relevance
 - An ability to prioritize the importance of events.
- **Improving system robustness & survivability**
 - An evaluation function that makes it able to respond meaningfully to adverse situations.
- **Our gained understanding of complexity and abstraction tradeoffs is a fundamental accomplishment**
 - Other MA projects may succeed or fail based on what we learn.
- **Prototype solutions to sponsor relevant systems that will lead to transition opportunities**
 - Level of prototype complexity approaches real sponsor needs.

Future Plans



- **Have settled on mission-thread modeling approach.**
- **Have developed and demonstrated performance impact prediction techniques on a small mission-system.**
- **Now modeling a Time Sensitive Targeting mission thread in detail**
 - **Identifying the IT infrastructure supporting the mission**
 - **Characterizing Mission MOEs and MOPs**
 - **Identifying mission role(s) to be informed by our system.**
- **We will formalize our methodology, develop a working prototype and also software tools that will make “mission impact assessment” a practical technique for wide-spread use.**
- **We will extend our approach to include the automated evaluation and selection of potential response actions that would mitigate attack effects in the context of maximizing mission success.**