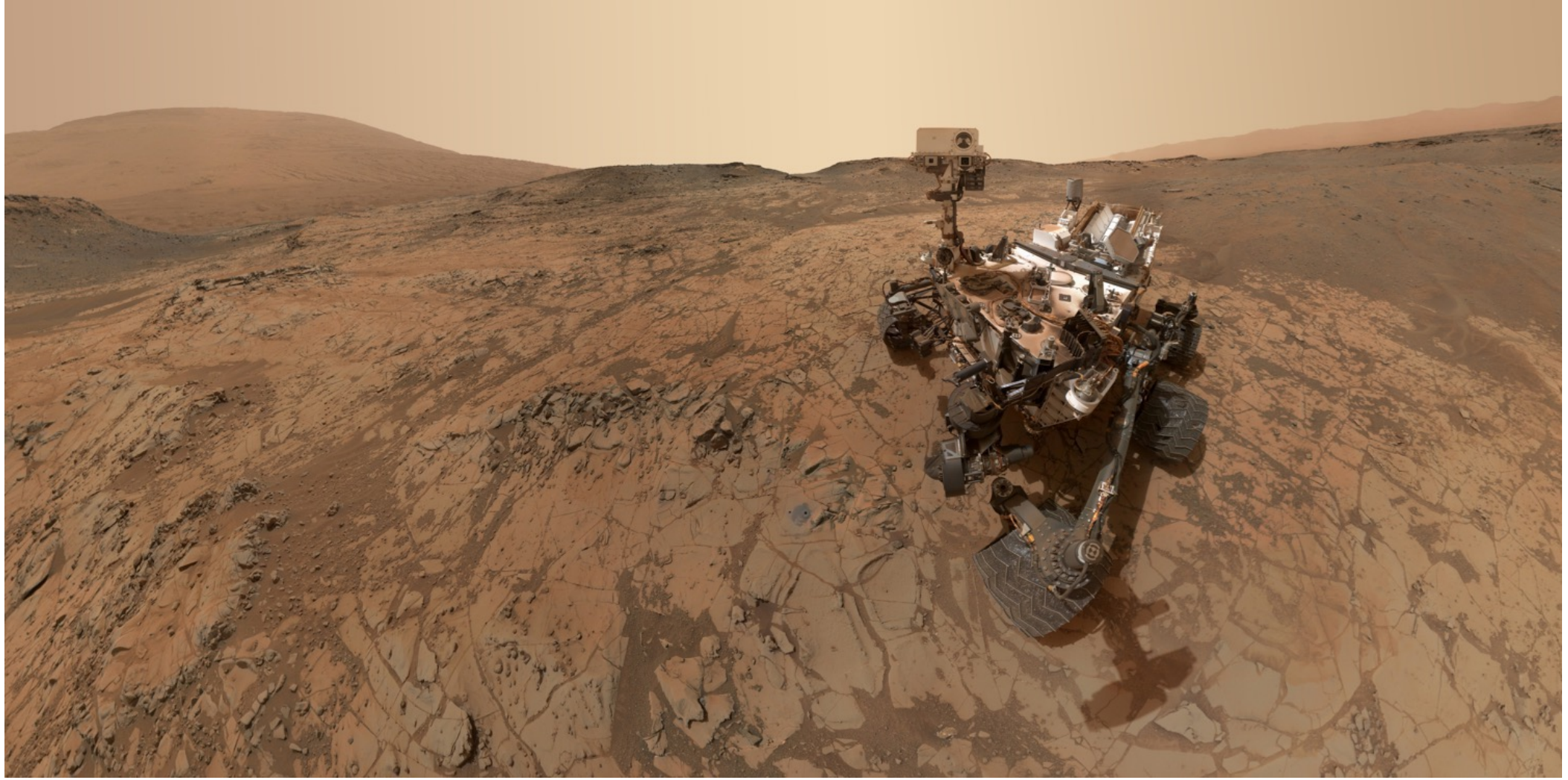


Defending space missions: Cybersecurity experiences from JPL operational deployments

Dr. Kymie Tan, Chief Cybersecurity Engineer

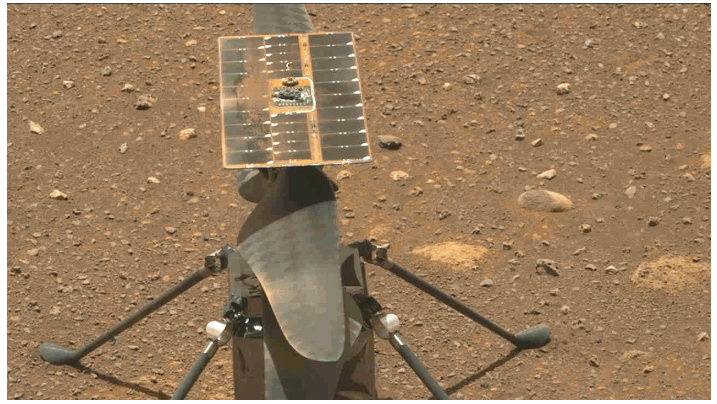
Cyber Security Experimentation and Test Conference, August 8th, 2022

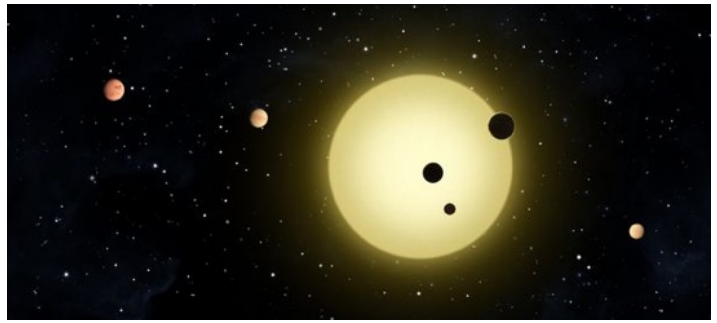
Jet Propulsion Laboratory
California Institute of Technology

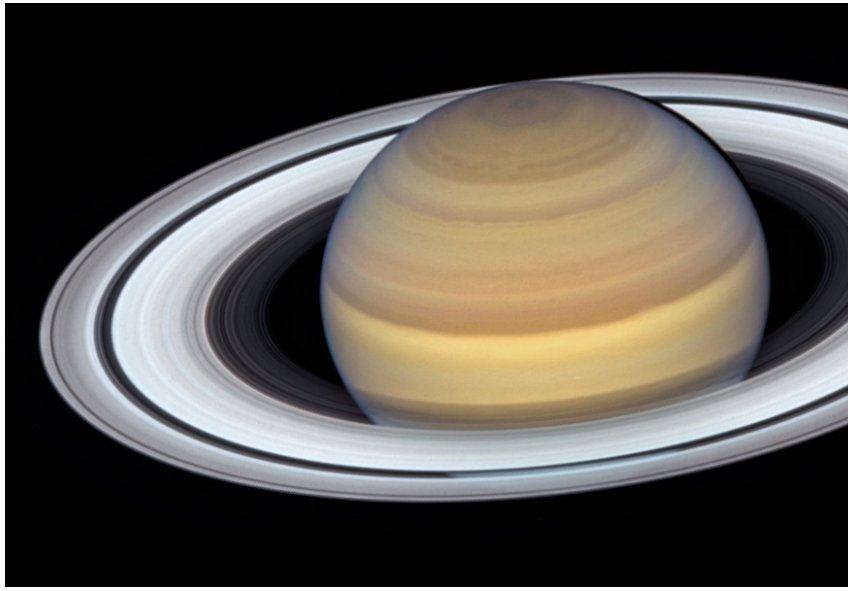
JPL'S MISSION FOR NASA

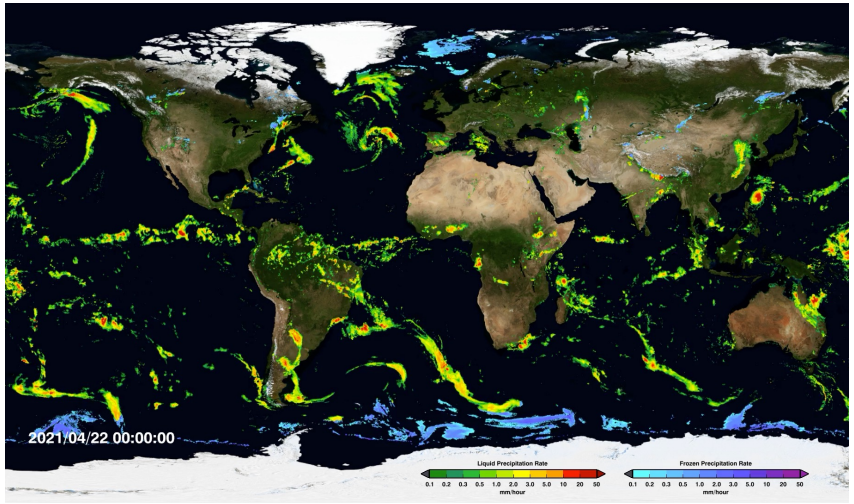
Robotic Space Exploration

Mars
Solar System
Exoplanets
Astrophysics
Earth Science
Interplanetary Network









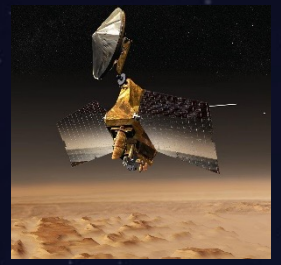
JPL is part of NASA and Caltech

- **Federally-funded** (NASA-owned) Research and Development Center (FFRDC)
- **University Operated** (Caltech)
- **$2.5-3.0B Business Base**
- **6,000 Employees**
- **167 Acres**
- **139 Buildings; 36 Trailers**
- **673,000 Net Square Feet of Office Space**
- **906,000 Net Square Feet of Non-Office Space**

Examples of Spacecraft and Instruments Across the Solar System and Beyond

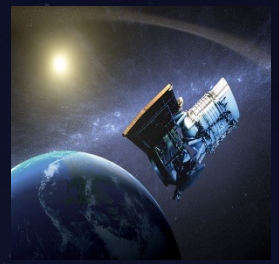
Two Voyagers (1977)

Mars Odyssey (2001)



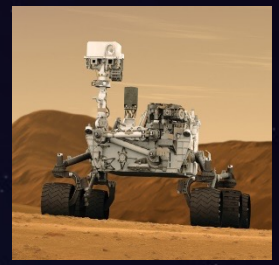
Mars Reconnaissance Orbiter (2005)

CloudSat (2006)

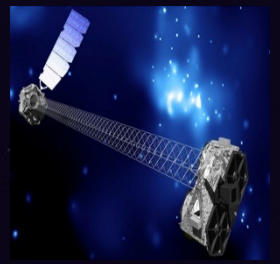


NEOWISE (2009)

Juno (2011)

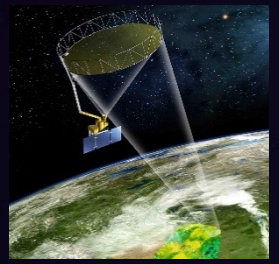


Curiosity (2011)



NUSTAR (2012)

OCO-2 (2014)

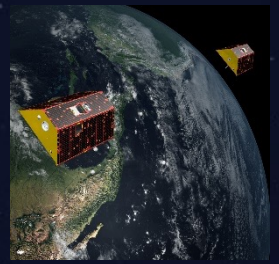


SMAP (2015)

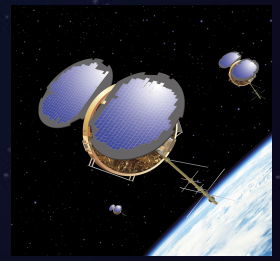
Jason 3 (2016)

InSight (2018)

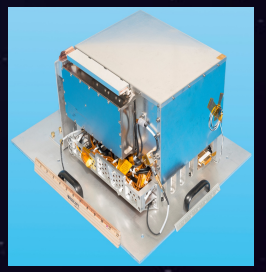
TEMPEST (2018)



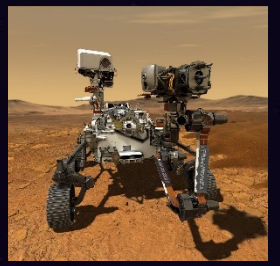
GRACE Follow-On (2018)



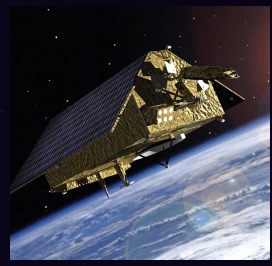
COSMIC-2 A (2019)



DSAC (2019) (1)



Perseverance (2020)



Sentinel-6 Michael Freilich (2020)

Instruments

Earth Science

- MISR (1999)
- ASTER (1999)
- AIRS (2002)
- MLS (2004)
- ECOSTRESS (2018)
- CAL (2018)
- OCO-3 (2019)
- HAWC+ on SOFIA (2016)

Planetary

- MARSIS (2003)

MISSIONS

Europa Clipper

SCIENCE SUMMARY

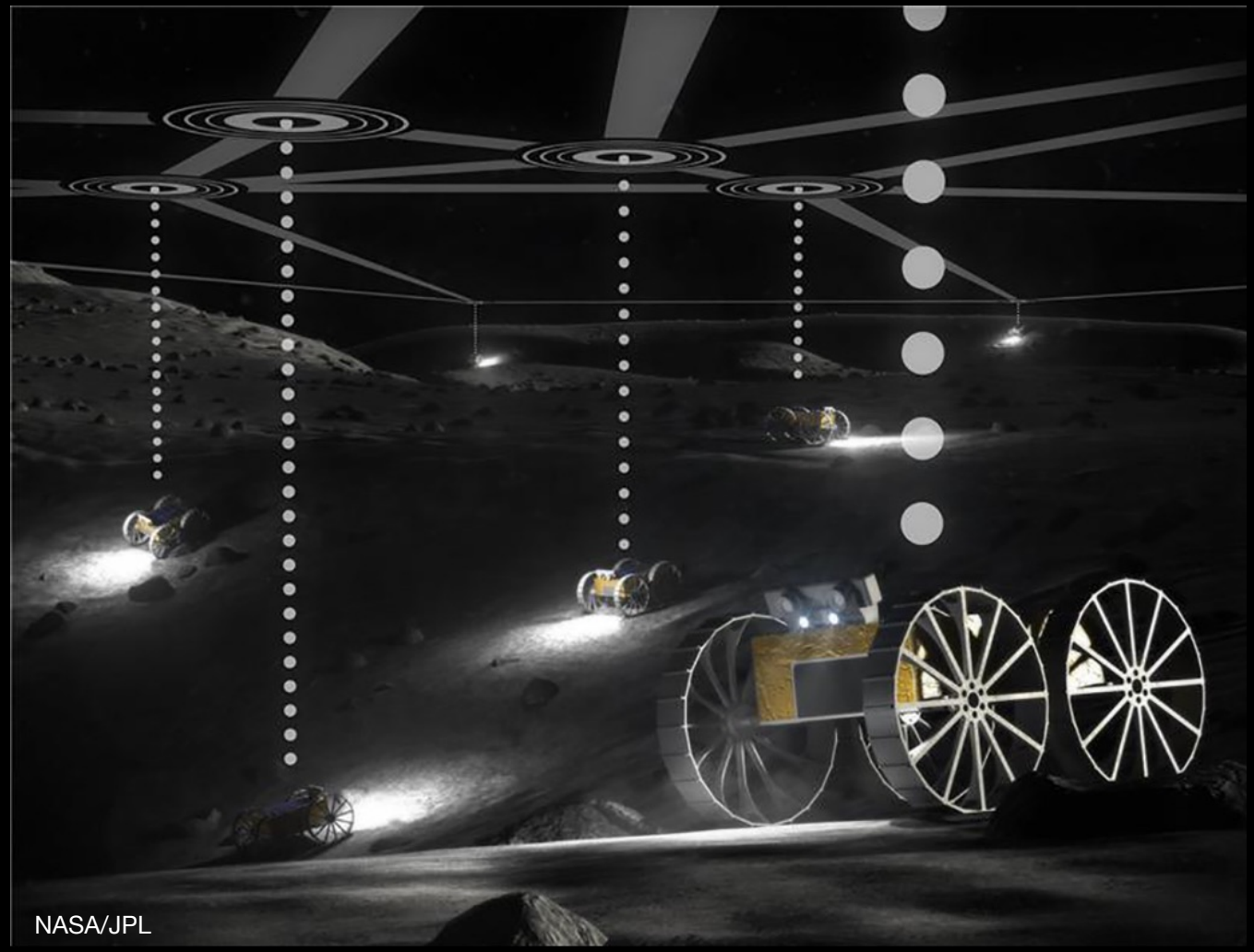
- Europa Clipper will conduct detailed reconnaissance of Jupiter's moon Europa.

- Clipper will investigate whether the icy moon could harbor conditions suitable for life.

xobiology Extant Life Surveyor (EELS)
echnology Development Program

Artists Concept

CADRE Multi-Agent Autonomy
Lunar Tech Demo Mission



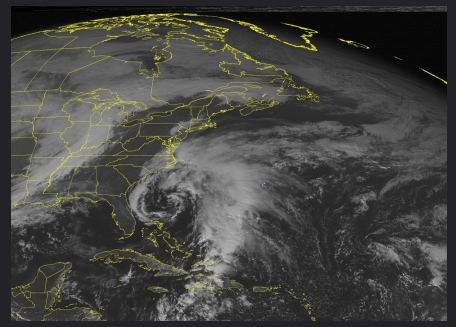
Cybersecurity in Space Missions

Cyber Incidents: Aerospace Systems

April 2005[1] – A rogue program penetrated NASA KSC networks, gathered data from computers in the Vehicle Assembly Building, and exfiltrated it through covert channels.

May 2011[2] – a hacker "TinKode" gained access to information contained on servers for the satellite-based Earth observation system

September 2014[3] – Chinese hackers breached computer networks to distort operational data coming from NOAA satellites.



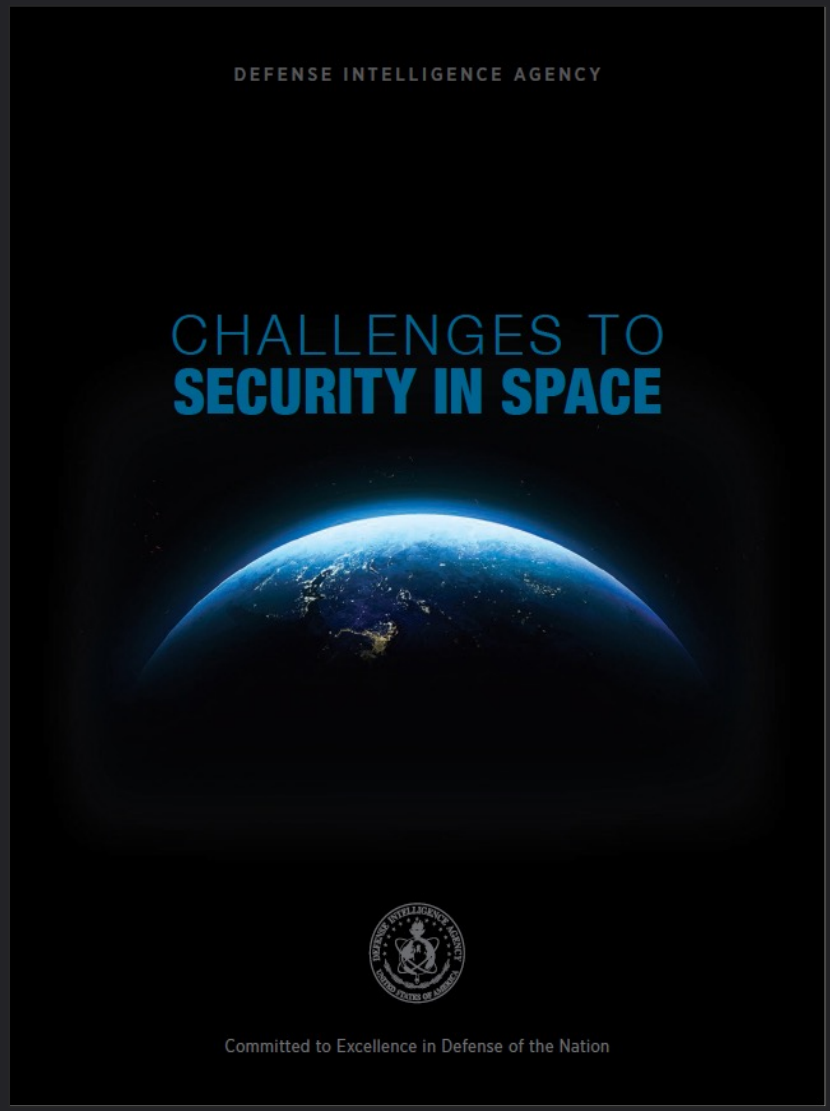
January 2016[4] – GSFC, GRC, and AFRC. Drone data and command authority hack.

April 2018[6] – compromised JPL external user account used to access mission systems

February 2022[6] –attack on an American company, Viasat, using malware ("Acid Rain") that resulted in significant communications loss for the Ukrainian army.

Cybersecurity Challenges to Space Missions

- **Legacy systems and components**
  Space systems have long operational life, with component lifetimes expected to last decades
- **Complex networked environments**
  Connected, interdependent system-of-systems
- **Long development times**
  Plenty of opportunities for early supply chain attacks
- **Fragile/limited redundancy**
  Currently not designed for defense against cyber attacks
- **Global supply chains**
  Open source software, parts developed overseas
- **Misconceptions/Assumptions about space system architectures**
  - Space systems are built using unique hardware/software that is not susceptible to common computer malware
  - Spacecraft only communicate only with ‘air gapped’ infrastructure
  - Once launched, the cyber risk to a space system is minimized
- **Workforce limitations**
  Spacecraft/mission systems experts are generally not the same experts that understand cybersecurity



Careful experimentation and measurement is critical to the operational viability of a cyber defense technology on space missions.

A Clash of Two Cultures

- Deploying a cybersecurity detector on space mission systems

- Mission system: Ground – telemetry
- Intention: Use an anomaly-based detector to identify off-nominal events
- Test program - needed:
  - Data feeds (“ground truth” data)
    - Nominal (background) data
    - Attack injected data
  - Server to deploy the detector
  - Set of critical applications to monitor
- “Hypothesis” – Detector will detect a set of attacks A using input data streams I, and produce outputs O with accuracy AC and precision P.

A Clash of Two Cultures -2-

- The response from JPL's Ground Data Systems Engineer

- **Questions …….**

A Clash of Two Cultures -3-

- The response from JPL's Project Systems Engineer....

- **Systems Engineering Questions**
  - What is the architecture of the system you expect the detector to operate it?
    - What architecture is required to ensure optimal performance?
      - Concerns with blocking/delaying elements? Firewalls, system configurations, etc.
      - Positioning constraints – require proximity to software/hardware elements?
      - Need to evaluate what the key characteristics of the deployment architecture are that will affect detector performance
    - What is the security architecture for the technology itself? E.g., meta-data repositories – encrypt?

  - What failure modes are expected? Have you designed test regimes for identifying and evaluating these failure modes? E.g., insufficient CPU, memory and disk resources for nominal detector operation

  - Who are the end users?
    - Is the output of the technology is actionable by the expected end users? E.g. mission engineers, security analysts, system administrators

Summary of lessons learned

(If the desire is to use the technology in operations)

- **Simplicity**
  - Promotes clarity w.r.t. deployment requirements - maintenance and functional integration into operations environment
- **Transparency**
  - Better supports diagnostic functions, “explainability” of results, to identify what went wrong, to identify improvements and to promote the utility of the technology over time
- **Consistency**
  - ***Less focus on high scores*** **- prefer a less accurate but consistent/dependably functioning technology than a highly accurate one that introduces risk and uncertainty**
  - ***More focus on errors*** **- Encourage experimental design that promotes a strong understanding of the error profile and failures rather than on achieving high accuracy alone**
  - ***Understand deployment architecture*** **- Incorporate an understanding of the deployment environment and how that perturbs the function of the technology**
  - ***Attention to details*** **– Identification of experimental confounds, sources of uncertainty and reporting metrics**

Which problem did we tackle first?

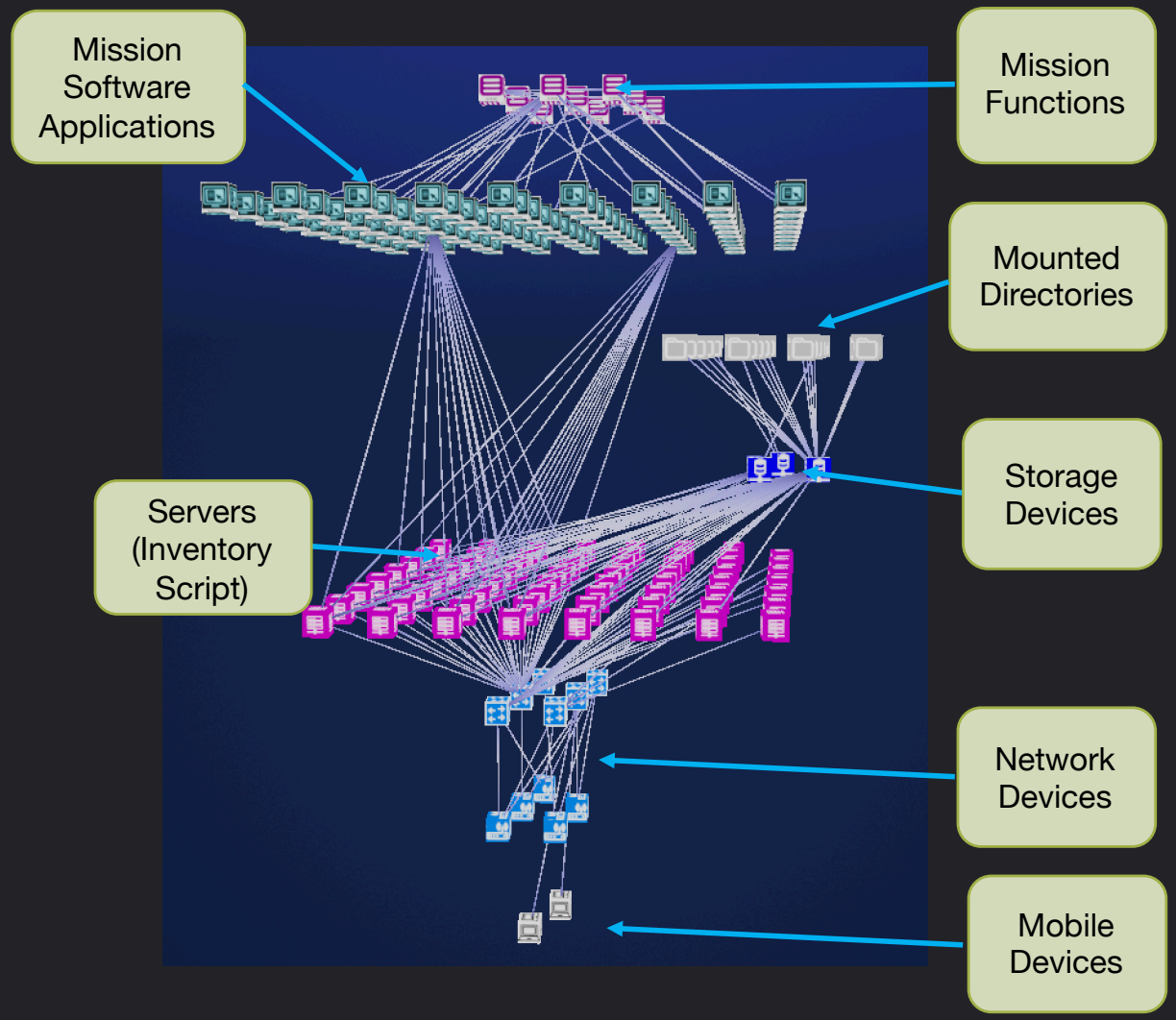
C.A.V.E

Cybersecurity Visualization and Analysis Environment

The Issues:

- Needed data
  - Different sources
  - Provenance
  - Documented characteristics – e.g., endemic anomalies (A.R.P. - Anomaly Resolution Process)
  - Etc.
- Needed architectural context
- Needed functional context – telemetry, commanding, ephemeris, etc.
- Needed to communicate with project engineers and managers
  - Projects need to rapidly understand the impact of an incident or potential adversarial incursion on mission objectives
- Need insights to plan response actions
  - Projects must provide evidence-based, reasoned responses to an incident or potential adversarial incursion

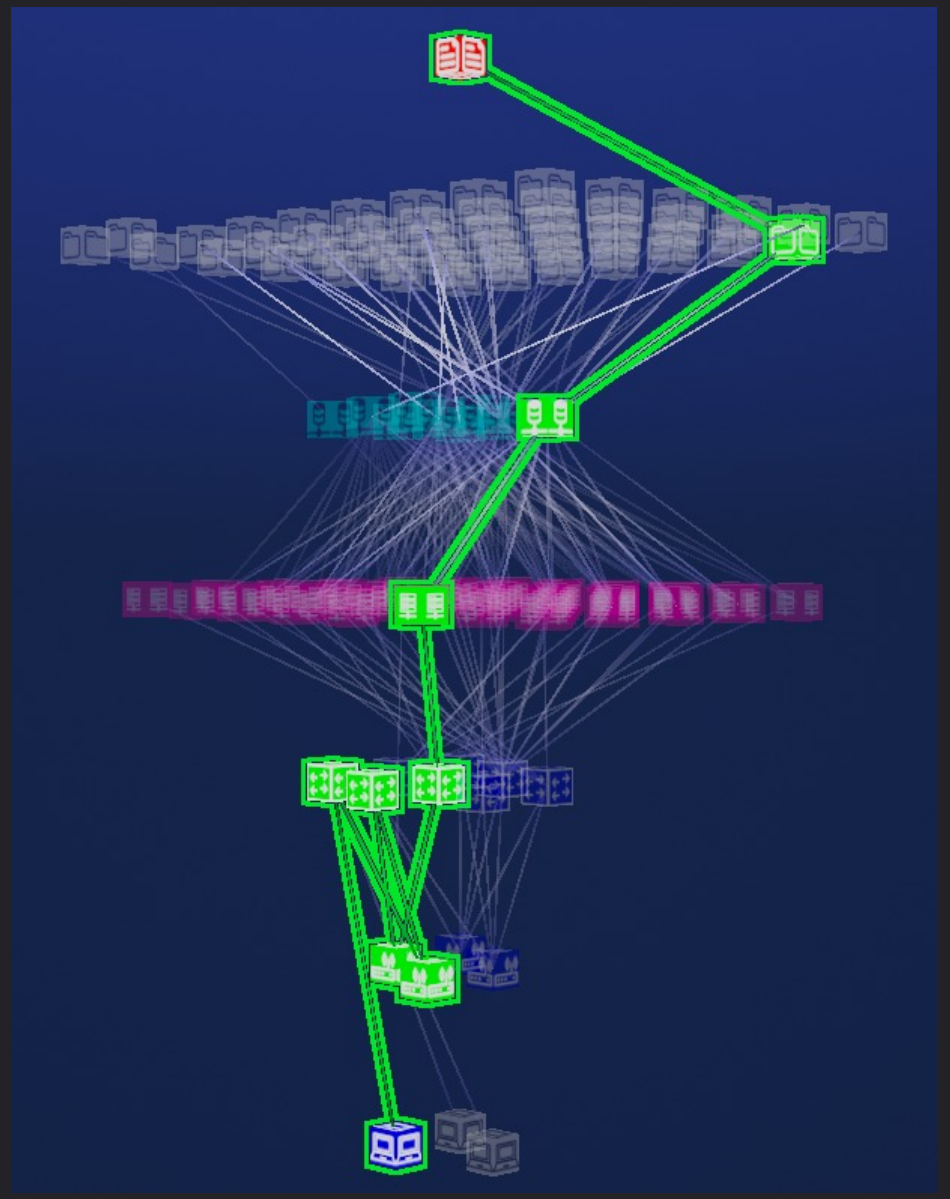
Cybersecurity Visualization and Analysis Environment



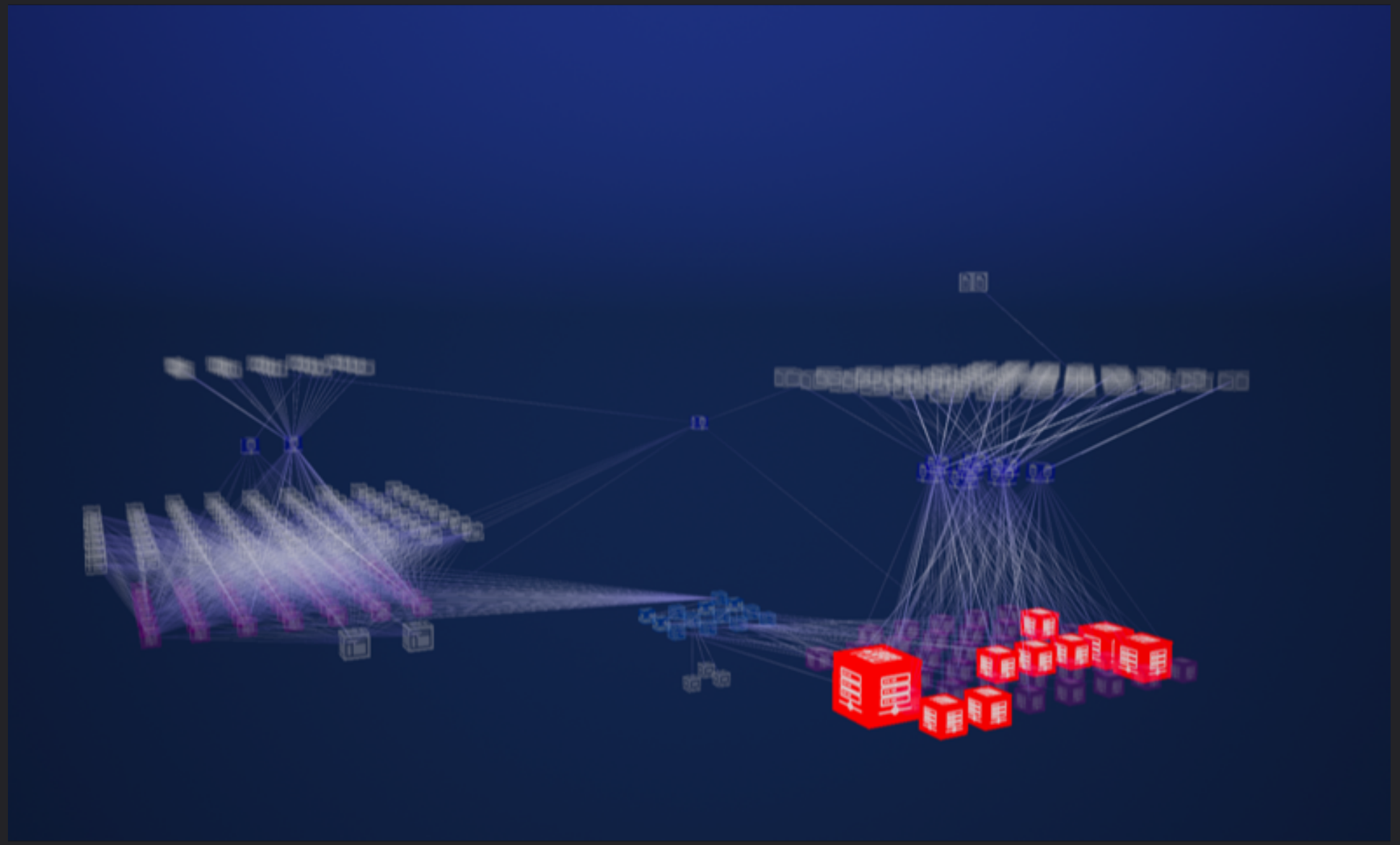
- JPL-developed, extensible, software framework to be used by mission and cyber analysts.
- Multi-layered cyber-physical system model
  - Hardware, software, files, processes, network connections, vulnerabilities , cost, risk
- Model-based reasoning
  - Determine consequences of adversarial activities to mission objectives
  - Report cyber-physical inventory to the mission
  - Track possible adversary entry/paths/goals given known weaknesses in our mission environment (i.e. CVEs, node centrality, proximity to the internet)
- Currently modeling missions in flight and development

Common questions asked by mission engineers…..

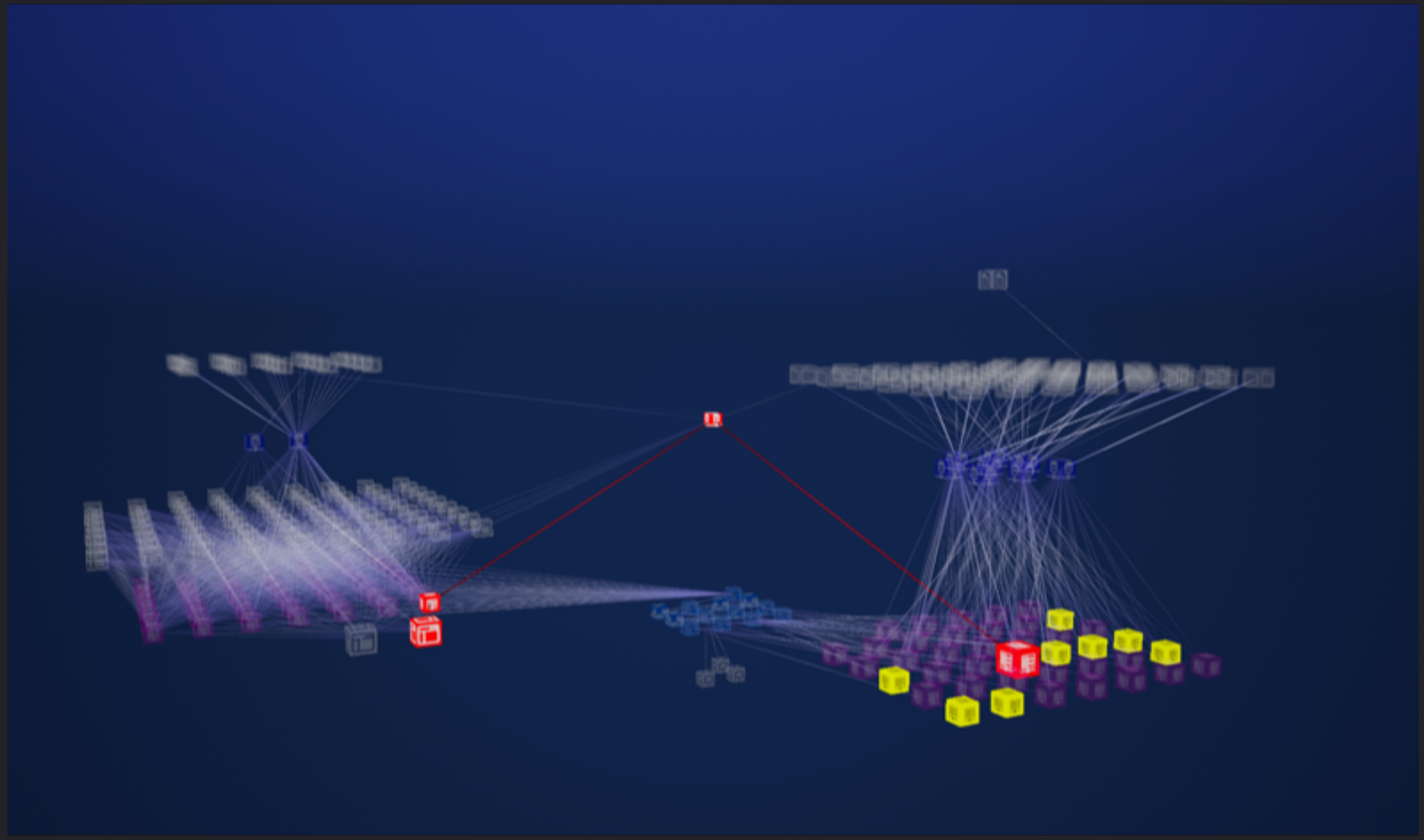
- On which ports can two servers communicate?
- What mounted directories can a server read?
- Are there any critical vulnerabilities on servers that can run a mission critical application?
- Which systems have a vulnerability with a downloadable exploit?
- Can an adversary access a critical mission resource from the internet?



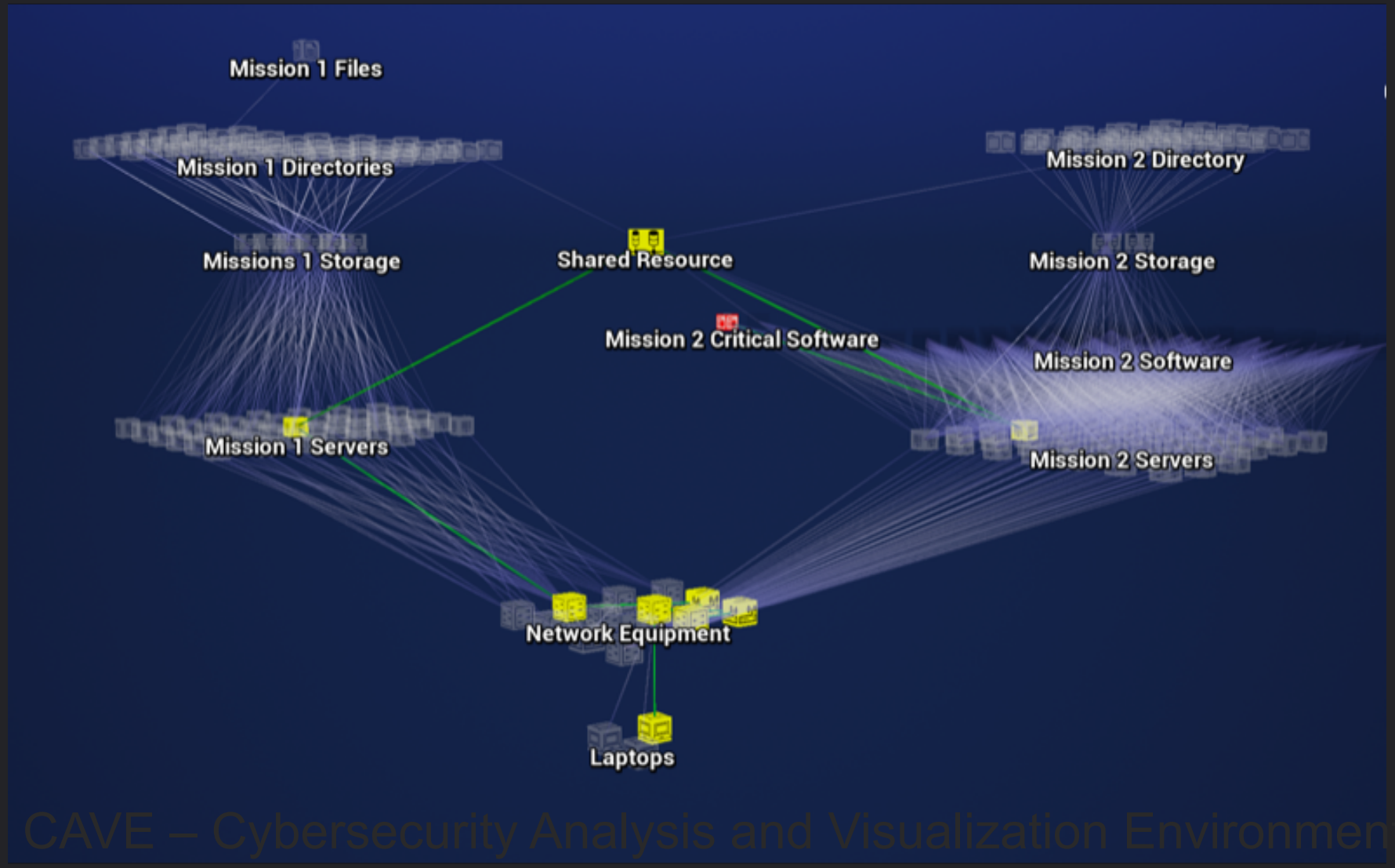
Prioritizing Remediation Actions



Prioritizing Remediation Actions -2-



Prioritizing Remediation Actions – Management View



In Summary .....

Operational deployment needs:

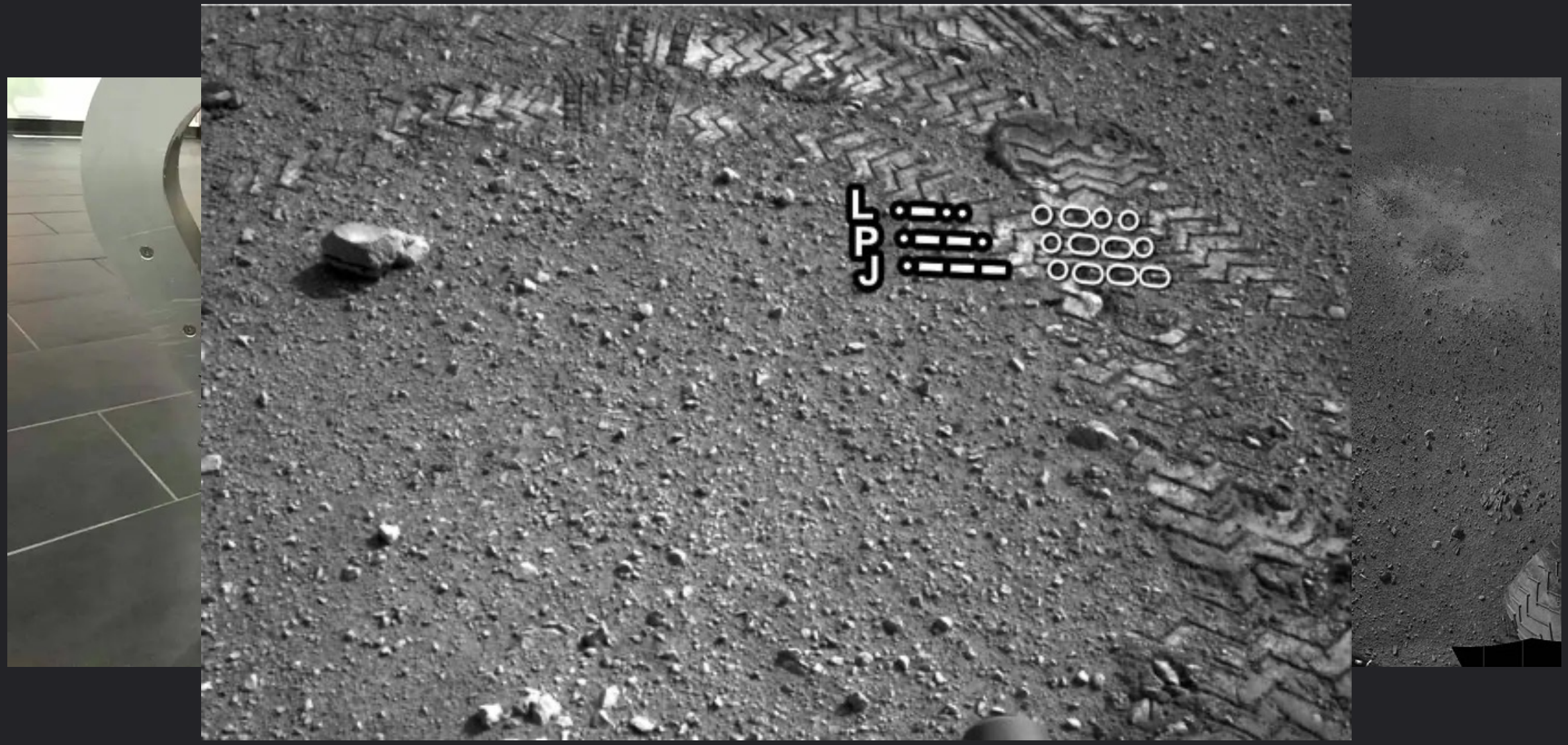
The ability to understand quickly

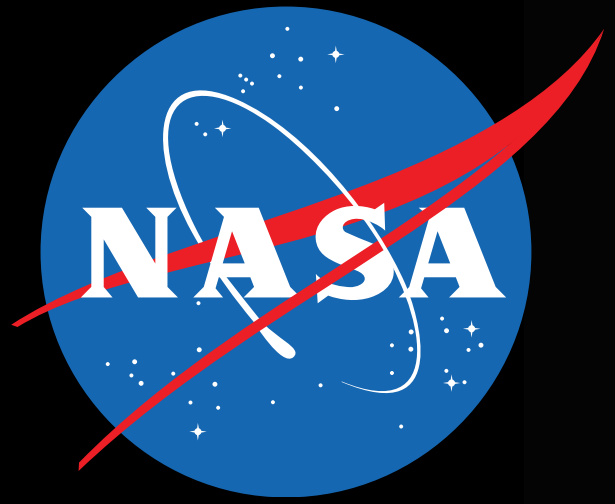
The ability to move quickly

- **Insights gained from analyzing failure and error profiles are invaluable in operations**
- **High-scoring technology is less desirable than dependably functioning technology**
- **Attention to details in experimental design – identification of confounds, sources of uncertainty and reporting metrics are important information that will drive the deployment approach**
- **The deployment environment/architecture and how aspects of that will perturb the performance of the technology should be considered**

Looking Forward to Future Missions

The Curiosity “Incident” – JPL Engineers at Play





JPL

A Clash of Two Cultures -2-

- The response from JPL's Ground Data Systems Engineer

- **Questions …….**
  - **Functional Questions:**
    - What quality of "ground truth" do you need? Can you characterize that for us?
      - Time granularity, event attribution (uncertainty tolerance), error tolerance profile, e.g., clock synchronization, etc.
      - Endemic anomalies – frequency, transmutation quotient
      - List of dependent variables mapped to each performance metric of the detector (see diagram)
      - Do you expect the system to explain its decision making (interpretability)?
      - If not, what artifacts in the test scenario do we need to allow an external observer to explain the decision making of the system (explainability)?