Scott Millwood

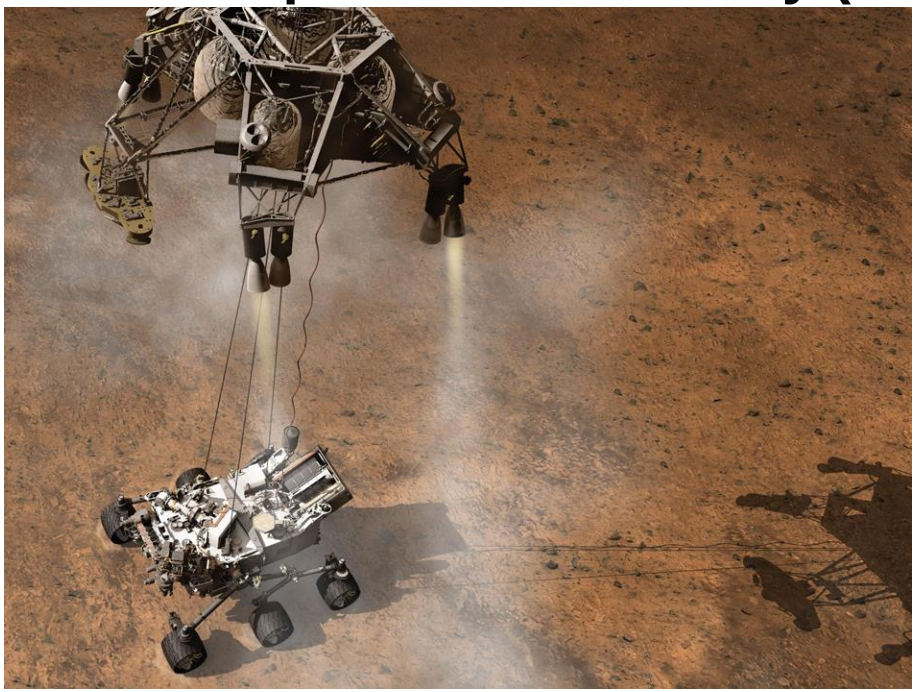
Secure World Foundation
Washington DC, 22 October 2019

Space and Cyber: Bolstering the Two Domains

CURIOSITY LANDS ON MARS

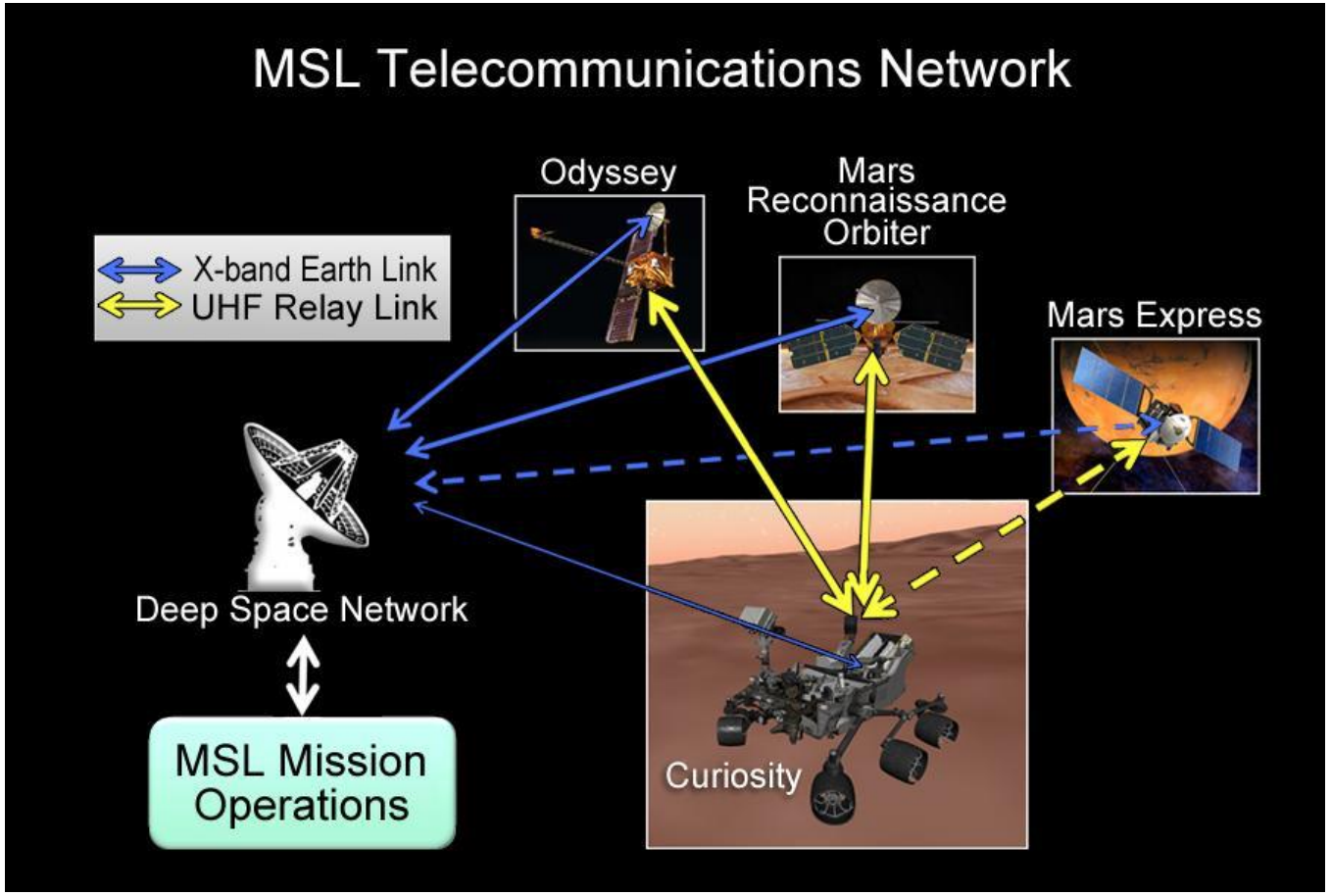
On 6 August 2012, **NASA's Curiosity Rover** landed on Mars, supported by the Mars Science Laboratory

at its **Jet Propulsion Laboratory (JPL)**



NASA has a contract with the **California Institute of Technology (Caltech)** to operate JPL's research on NASA's behalf, but **NASA retains responsibility for cybersecurity**

CURIOSITY RELAYS DATA TO EARTH



In the first 2 years after Curiosity's landing, orbiters supported the **downlink of 48 GB of data**

NASA CYBER BREACH 2018

In April 2018 it emerged that **an unauthorized user**, which had used an external user account to exploit weaknesses in Jet Propulsion Laboratory's cybersecurity controls, was able **to enter and operate undetected** inside the JPL network for **ten months** between 2017 and 2018

During this time the attacker extracted at least 500MB of sensitive mission data, **moving laterally** between systems, **exposing NASA data** to exploitation by cyber criminals

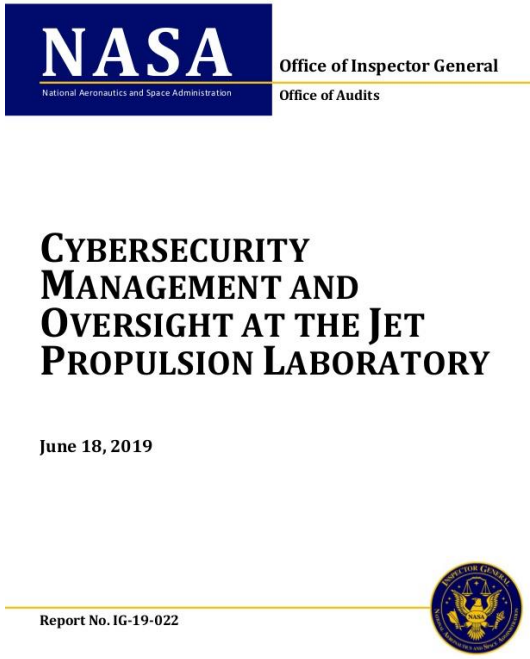
NASA Cybersecurity Audit 2019

In June 2019, NASA's Inspector General released the administration's audit report into the incident, identifying **multiple IT cybersecurity weaknesses**:

1. tracking of physical assets & applications in the network was **incomplete and inaccurate**, creating **a lack of visibility** of devices connected to it
2. gateway and databases had **not been segmented to limit user access only to those systems** for which they had approved access
3. failure to establish **security access agreements or protocols** with its partners and suppliers, specifying cybersecurity requirements to connect to NASA's IT systems
4. log tickets, identifying **cybersecurity vulnerabilities,** were not resolved for extended periods of time—sometimes longer than 180 days

NASA Cybersecurity Audit 2019

5. a lack of **technical tools** for monitoring unusual activity, such as Advanced Persistent Threats, **delayed identification** of the cybersecurity breach, **containment** of the incident and **eradication**
6. despite a major cybersecurity breach in 2011, in which cyber intruders gained full access to 18 servers supporting key JPL missions and stole 87 GB of data, NASA & JPL had **failed to implement learnings**
7. a lack of **system administrator responsibility**
8. a lack of **cybersecurity governance frameworks**



THE RELIABILITY OF DATA

The integrity of science requires reliable data

Most likely harmful interference with space activities is **technical** and the most vulnerable access points are **on Earth**

There are growing threats to critical infrastructure from **GNSS interference (spoofing)**

Establishing a **culture of cybersecurity governance** in the space sector is crucial

7 INSIGHTS

What Space Missions can learn from Cybersecurity Breaches

& Counter-measures in the Telecommunications Industry

INSIGHT #1

Data has a value

(so does a cybersecurity breach)

INSIGHT #2

Cybersecurity breaches tend to occur in the supply-chain

INSIGHT #3

Cybersecurity governance has evolved from “perimeter defense” to a risk-based holistic cybersecurity strategy with depth

(go beyond technical controls)

INSIGHT #4

Resilience requires a data culture

Cybersecurity = people + processes + technology

INSIGHT #5

Humans remain the most significant vulnerability

“This mission is too important for me to allow you to jeopardize it”

HAL9000 to Dave in Stanley Kubrick’s *2001: A Space Odyssey*

INSIGHT #6

Convergence will increase the risks

New players means new risks

Big Data & AI mean new risks

But not all data is equal

INSIGHT #7

Plan for the inevitability of cybersecurity breaches

Why is all of this important?

If a cybersecurity breach is any act that **interferes with the accuracy, integrity and reliability of data,** then the proliferation of **fake news and disinformation** seeking to confuse voters, can also be understood in these terms

Protecting our societies against interference
not only protects the integrity of science and our critical infrastructure,
but our democratic institutions

Scott Millwood