“I've been thinking about laws on Mars. There's an international treaty saying that no country can lay claim to anything that's not on Earth. By another treaty if you're not in any country's territory, maritime law applies. So Mars is international waters. Now, NASA is an American non-military organization, it owns the Hab. But the second I walk outside I'm in international waters. So Here's the cool part. I'm about to leave for the Schiaparelli Crater where I'm going to commandeer the Ares IV lander. Nobody explicitly gave me permission to do this, and they can't until I'm on board the Ares IV. So I'm going to be taking a craft over in international waters without permission, which by definition... makes me a pirate. Mark Watney: Space Pirate.”

Lecture Two

The Adversarial Mindset


Space
HACK THE PLANET

Targeting Space Systems

- Target Selection
  - What is the thing that is being attacked, how was it chosen
- Desired effect
  - What is the thing the attack looks to achieve

Motivation

- Collection
- Redirection
- Subversion
- **Theft**
- Disable

Target Selection

- Targeted based on opportunity
  - Known ability to access (vulnerability, supply chain interdiction, insider threat, etc.)
- Targeted based on who owns SV
  - Operated by a government or company the attacker wants to impact
- Targeted specifically
  - Space System targeted because of exactly what it is
- Targeted based on what SV does
  - Going after any space system with a certain mission or missions

Space Vehicle Types

- LEO
- MEO
- HEO ~Geo-stationary
- Non-Earth Orbital
- Non-Earth
- Deep Space

Targeting via Mission Type: Sensing

- Sensing missions
  - Radio Frequency (RF)
  - Optical
  - Infrared (IR)
  - Radiation

Targeting via Mission Type: Emitting

- Emitting missions
  - Interference
  - Injection
  - Laser
  - Navigation

Targeting via Mission Type

- Transit
  - Cargo
  - Passenger
  - Communications
  - Weapon

Targeted for Potential

- Software definition expands targetability
- Repurposing alters adversary cost benefit calculus
- Target because of what you could be
  - A Sensor becomes a jammer
  - A Comms payload becomes a listener
  - A transport (or anything big enough) becomes a weapon

Vectors

- Pre-Operational

- Operational

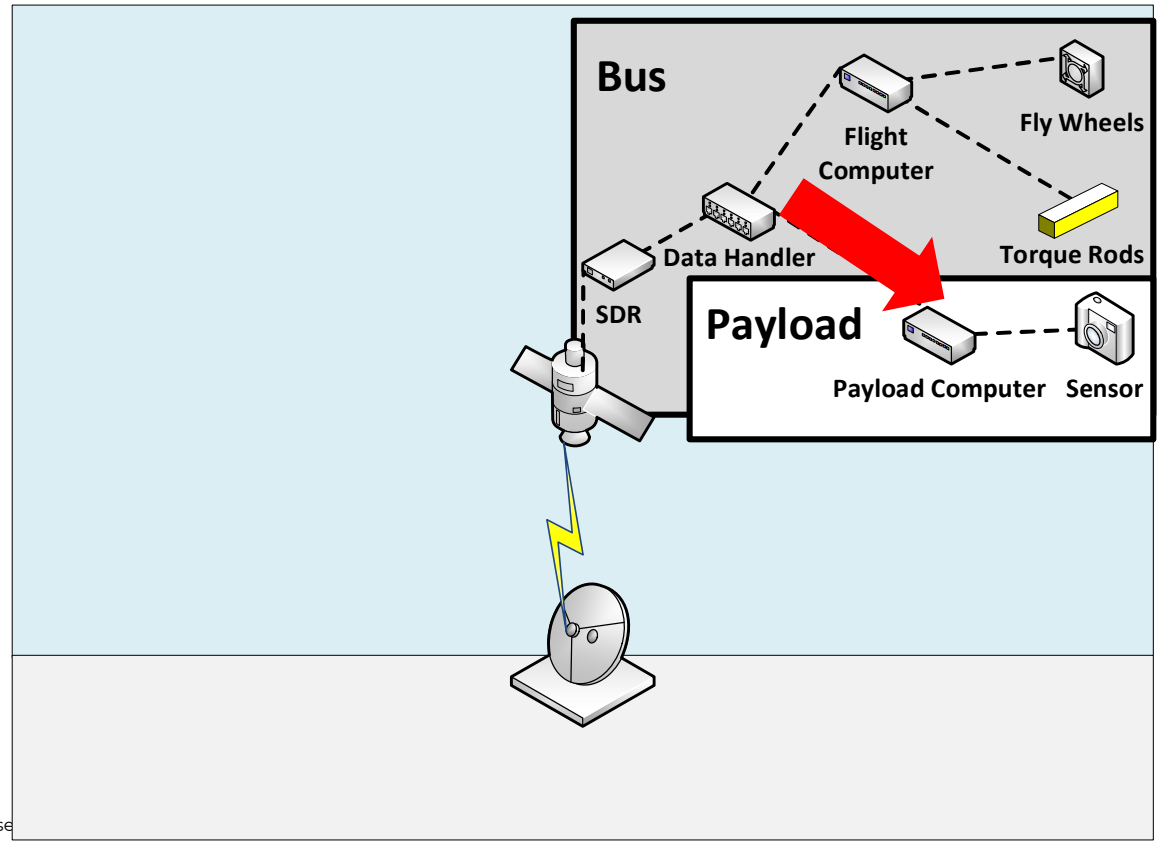
Pre-Operational Vector

- Design
- Development
- Testing
- Transportation
- Storage
- Launch

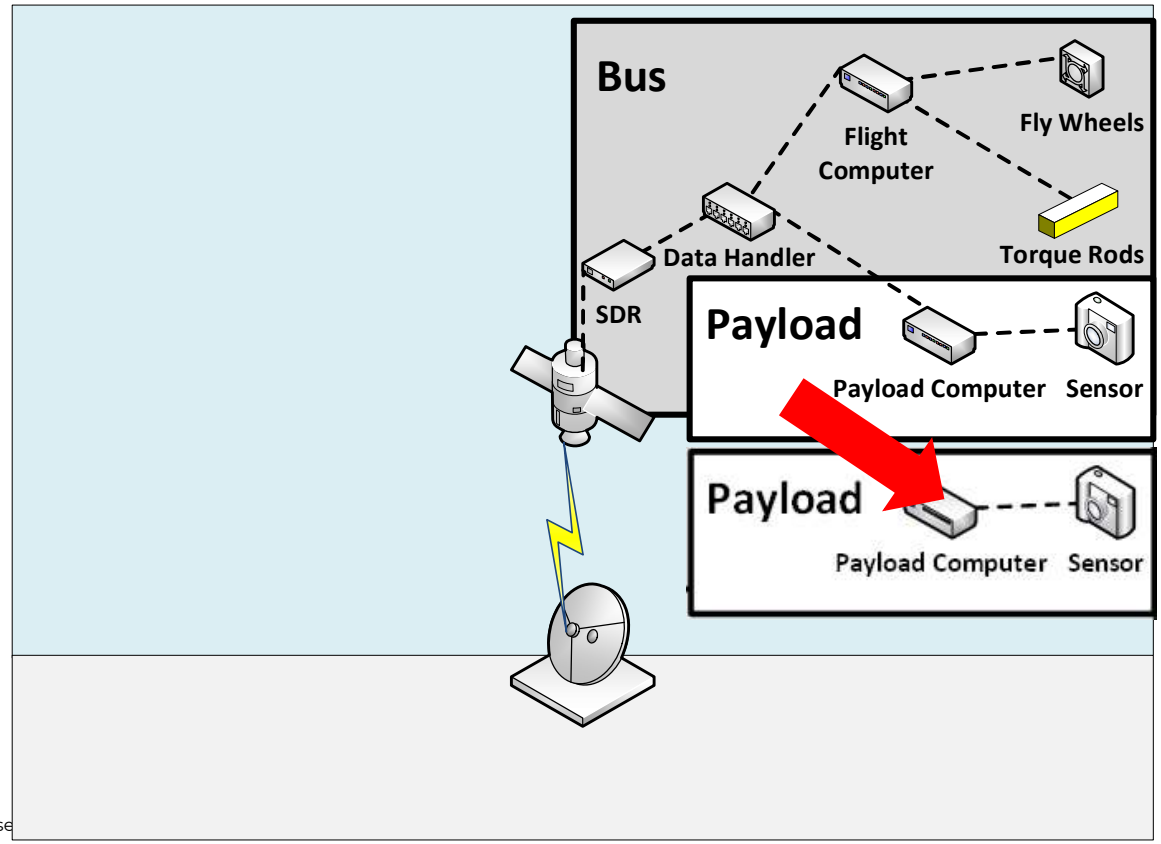
Operational Vector

- Ground / space link (both directions)
- Space links
  - Inter-vehicle
  - SV to SV
- Analysis & Dissemination
- Consumers / Customers

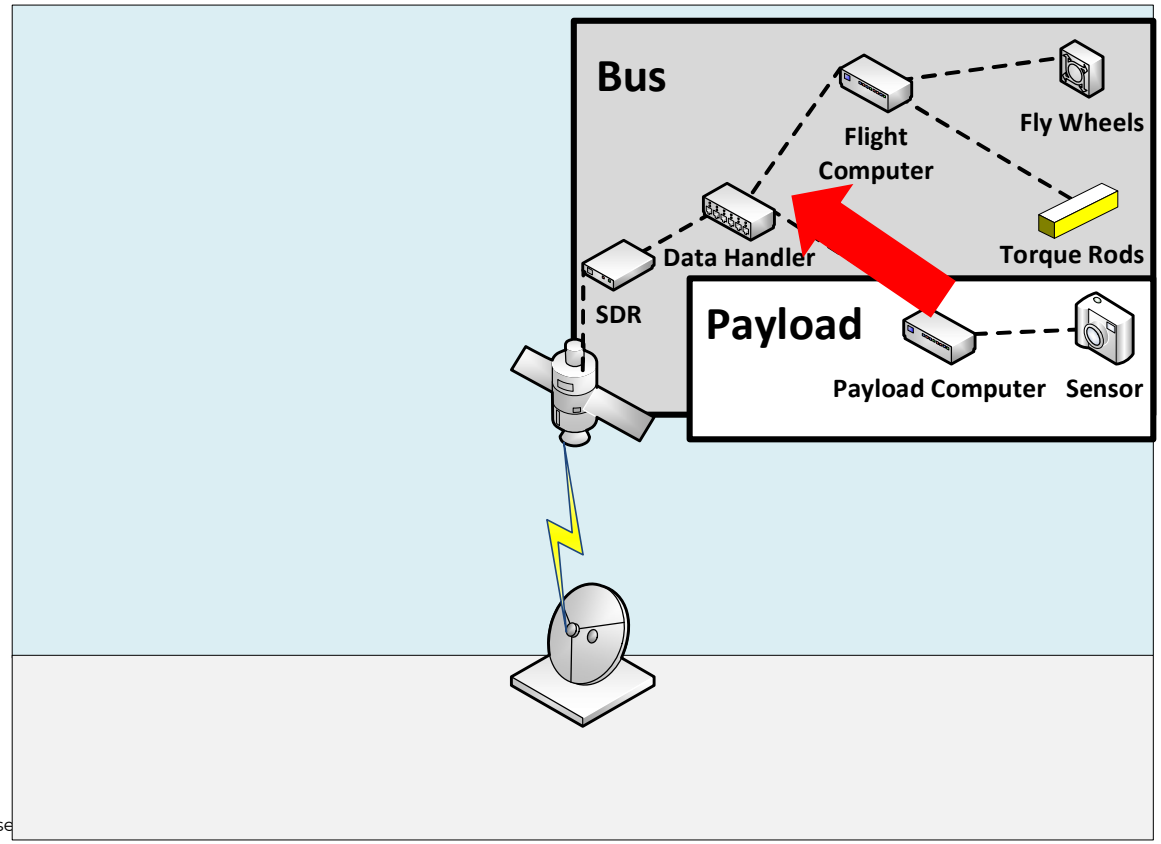
Bus to Payload



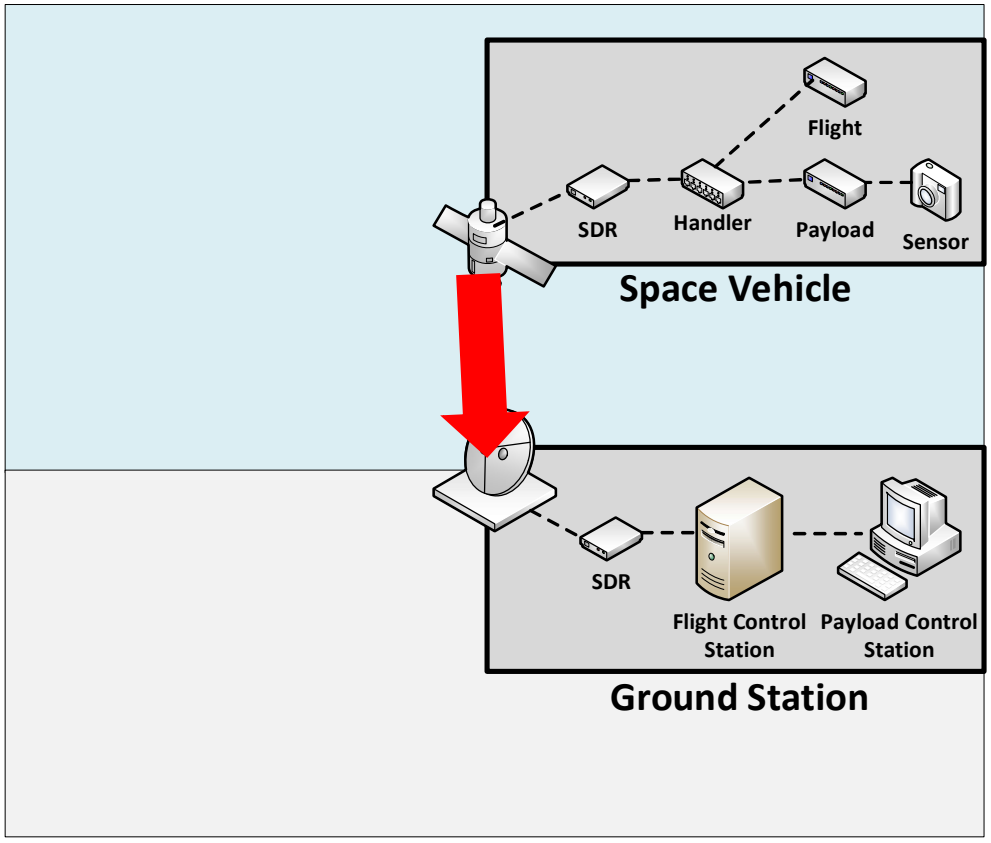
Payload to Payload



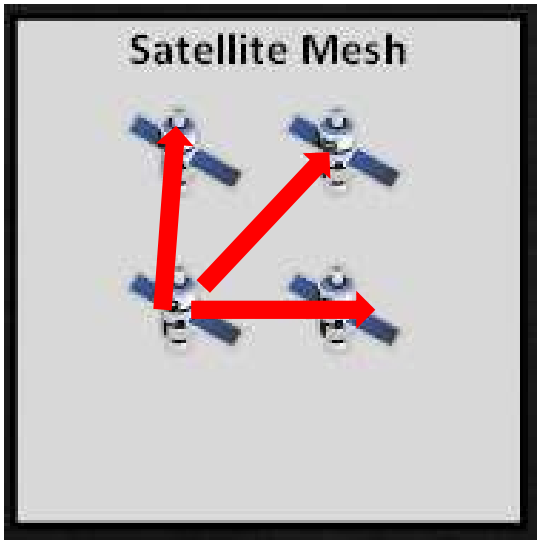
Payload to Bus



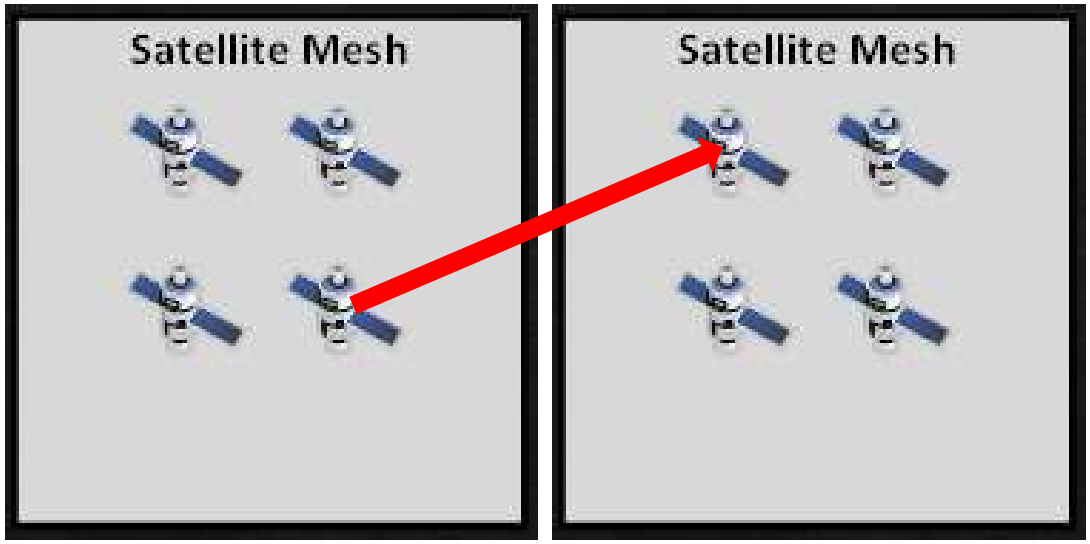
Space to Ground



Space to Space



Cross-Constellation



Exploitation

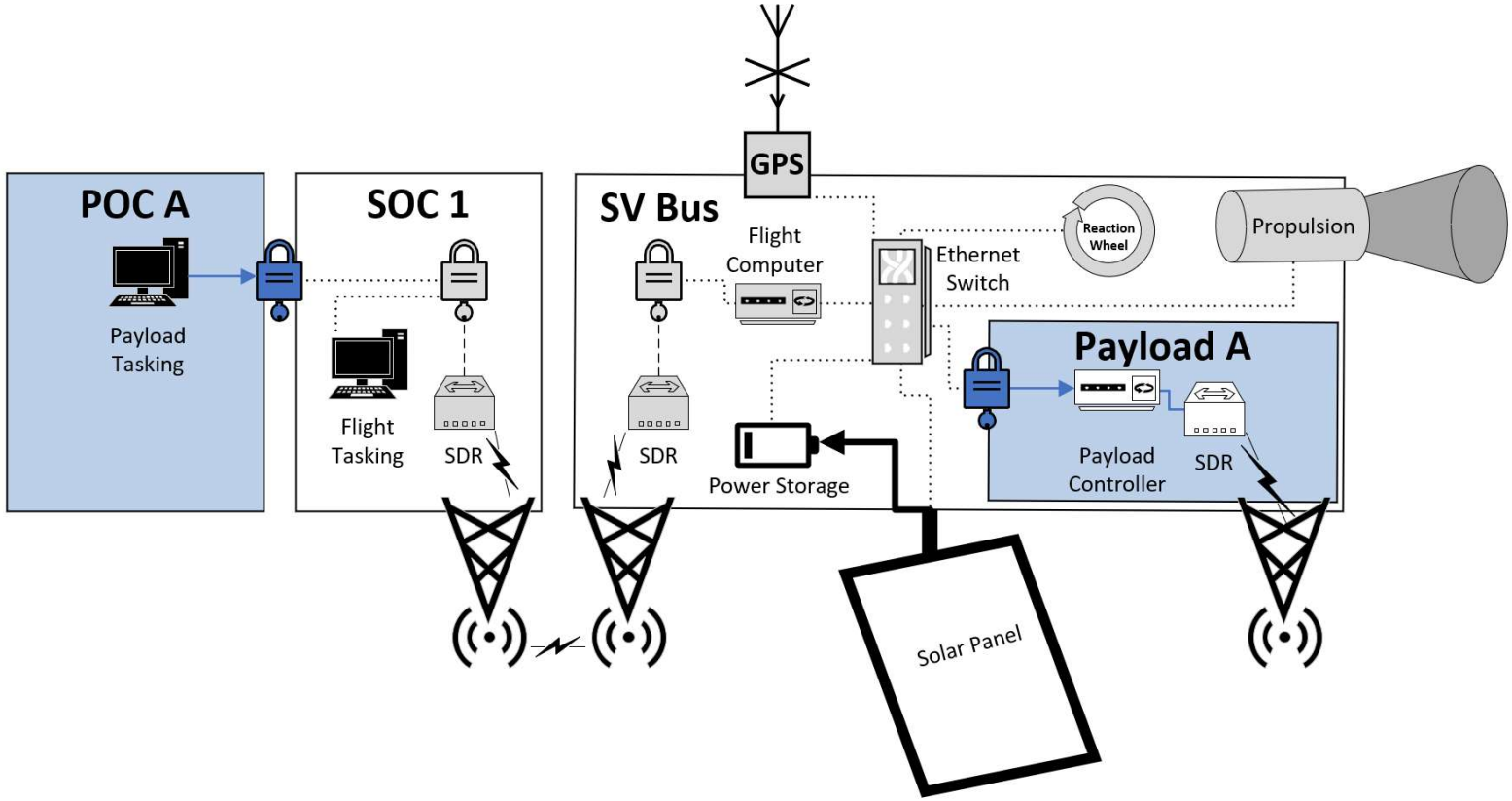
- Delineation between SV systems and mission systems is important in any non-integrated SV due to
- If ransom is goal, may take whichever you can access, be it hosted payload or bus
- If collection is goal, may have to be payload side
- If disabling the SV is goal, may have to be bus side

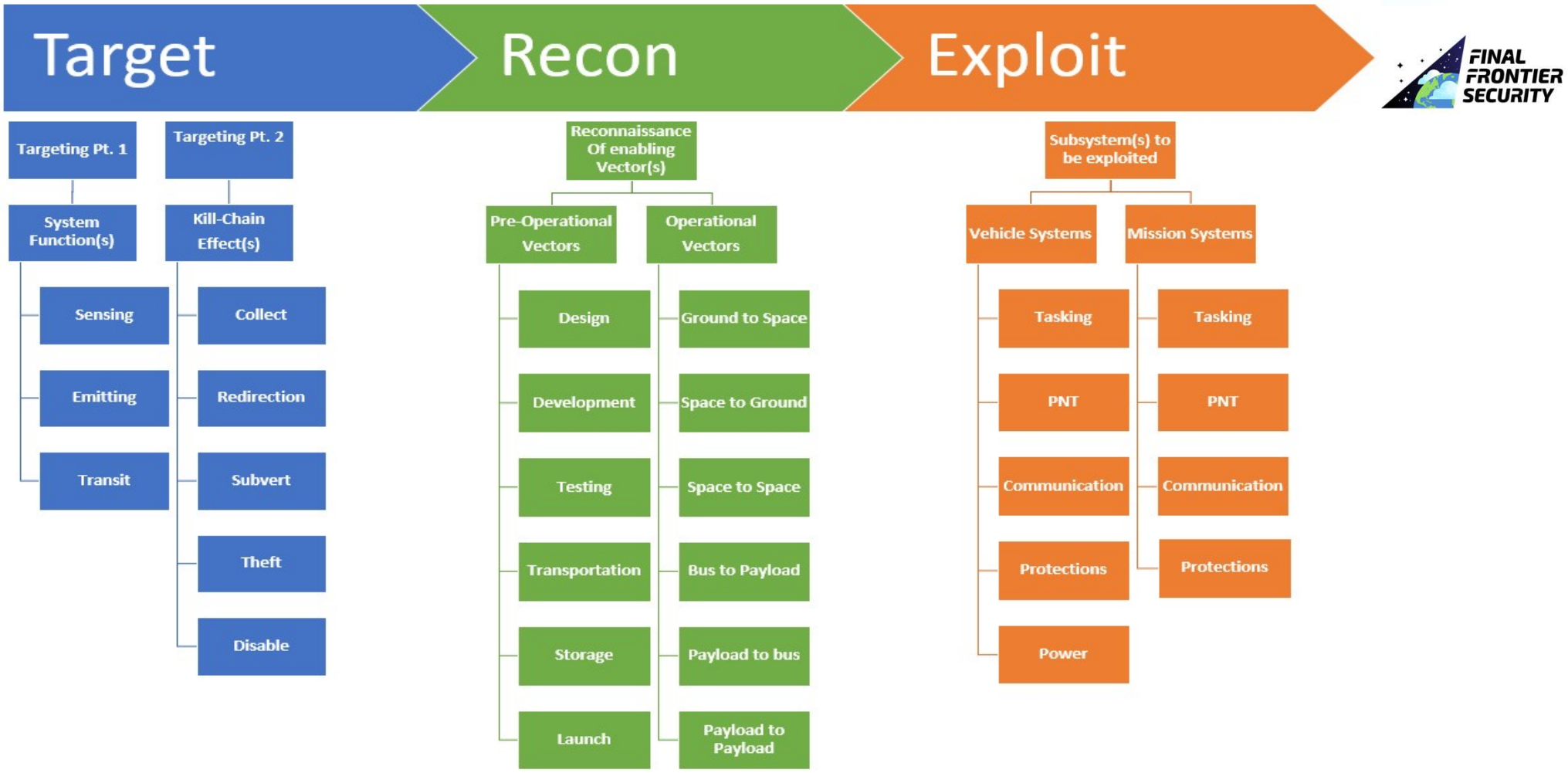
Subsystems to Exploit

- Bus and Payload Subsystems
  - Tasking (receiving, executing, storing)
  - PNT knowledge
  - Communications
  - Protections (resource limiters, watchdogs, etc.)

- Bus specific subsystems
  - Power (generation, distribution, storage)
  - Attitude

Subsystems to Exploit Illustrated





Tradecraft Considerations

LEO Constraints

- Persistent vs non-persistent communications
- Orbital implications
- Constellations, meshes and formation flying

Asynchronous Satellite Operations

- Tasking ahead
- Prioritization of commands
  - Station keeping vs power generation vs mission etc.
- Impacts of automated SV activity
  - Watchdogs and resource limiters
- Predicting availability and usability

Asynchronous Cyber Operations

- Operating in the blind
- Working without guaranteed communications
- Troubleshooting challenges
- Dynamic operations
- Tradecraft implications

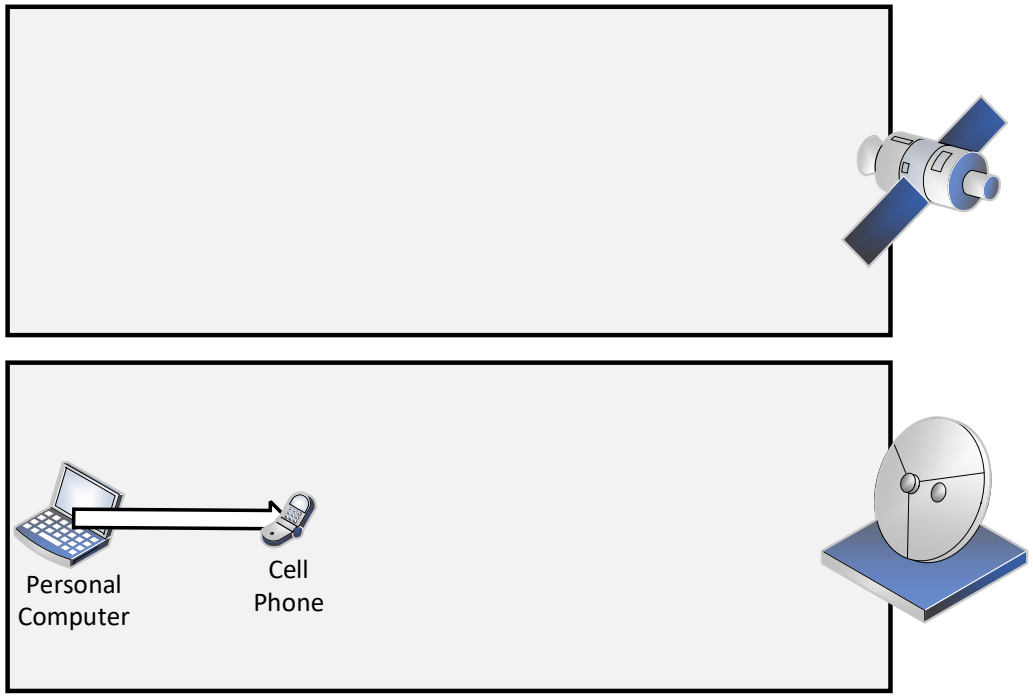
Pivoting

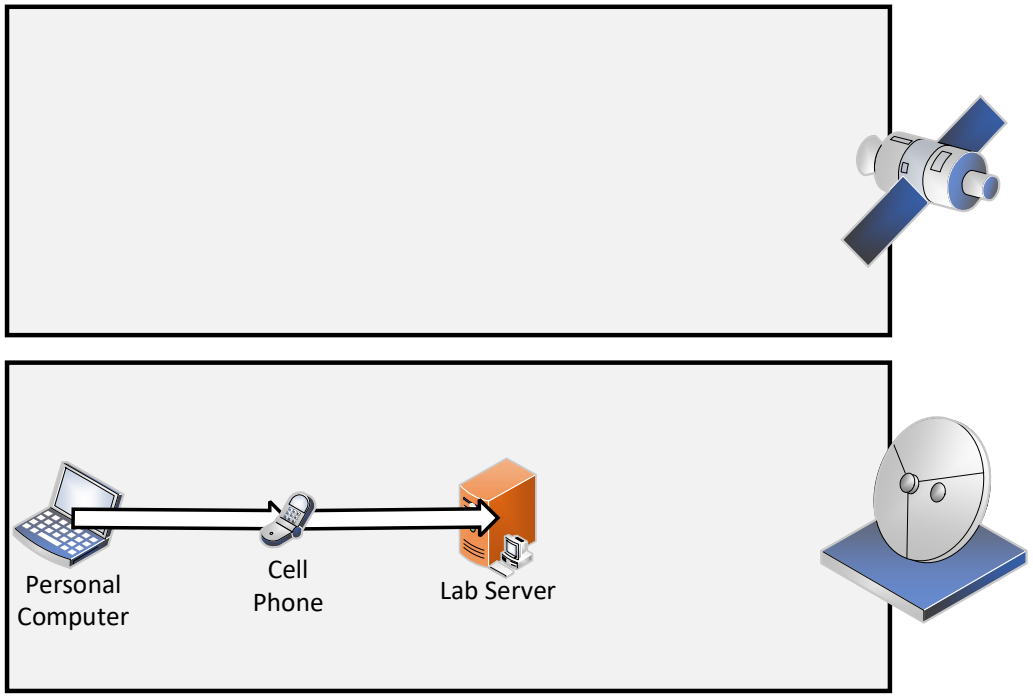
- Ground to Space
- Inter-Bus
  - Bus to Payload
  - Payload to Payload
  - Payload to Bus
- Space to Space
- Space to ground

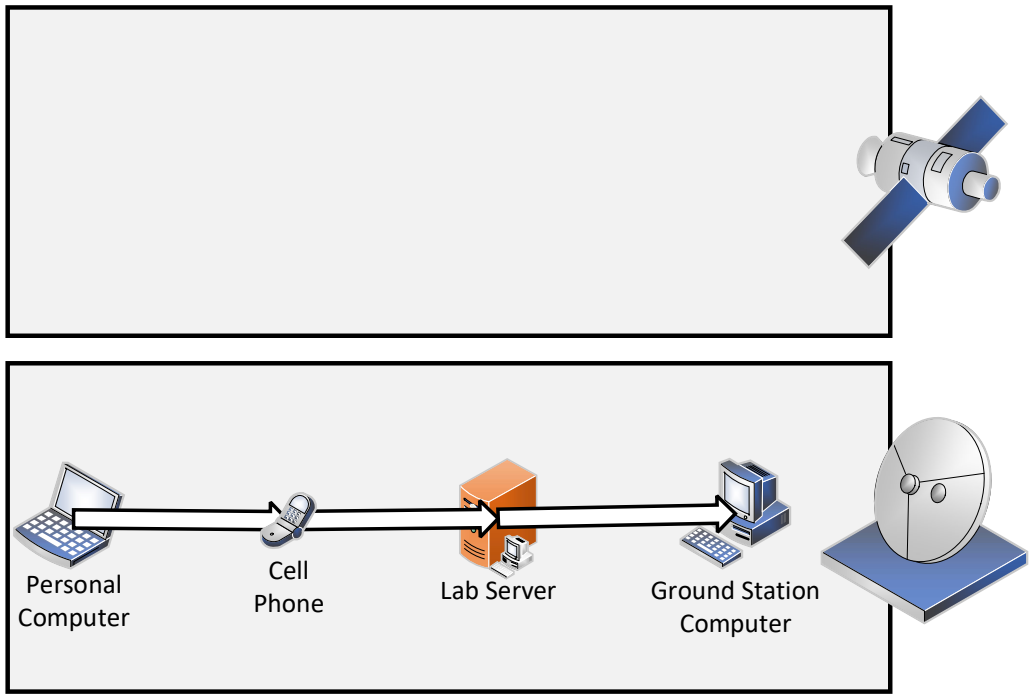
SV Code Execution

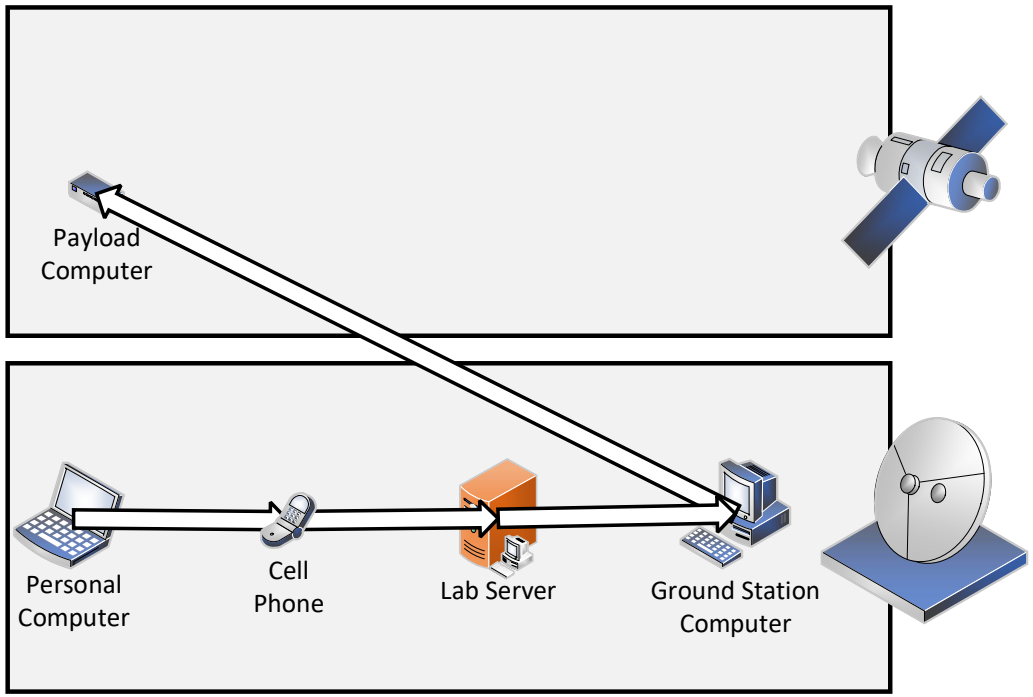
- Living off the land
  - Tasking updates
  - Abusing watchdogs like scheduled tasks?
  - Registering your own apps
- IOCs
- Getting caught or killed by redundancy mechanisms

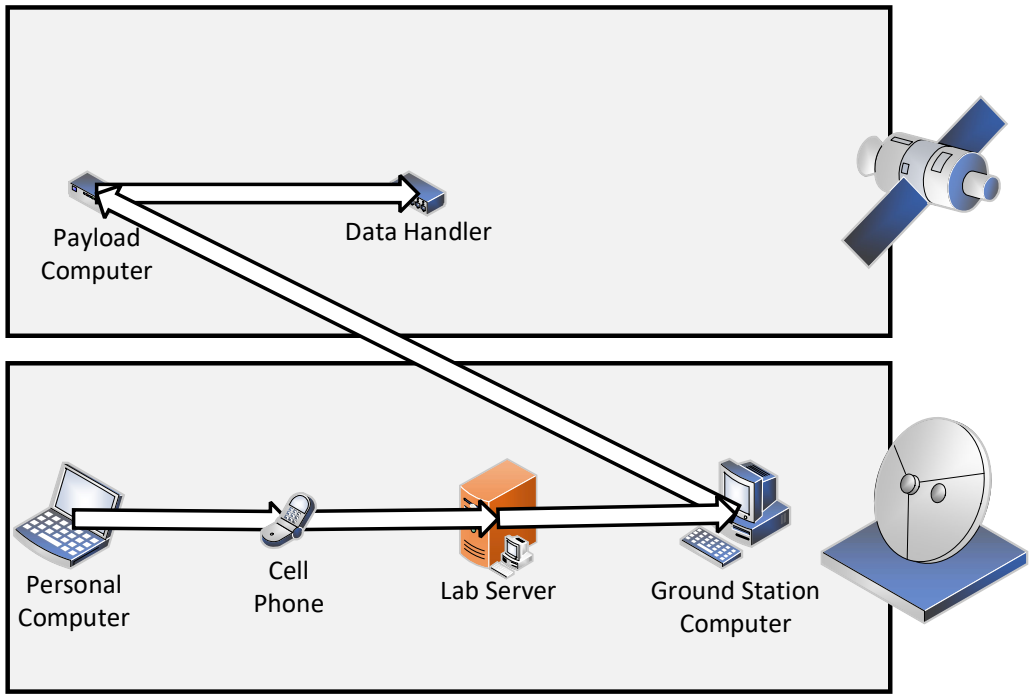
Realistic Compromise Scenario

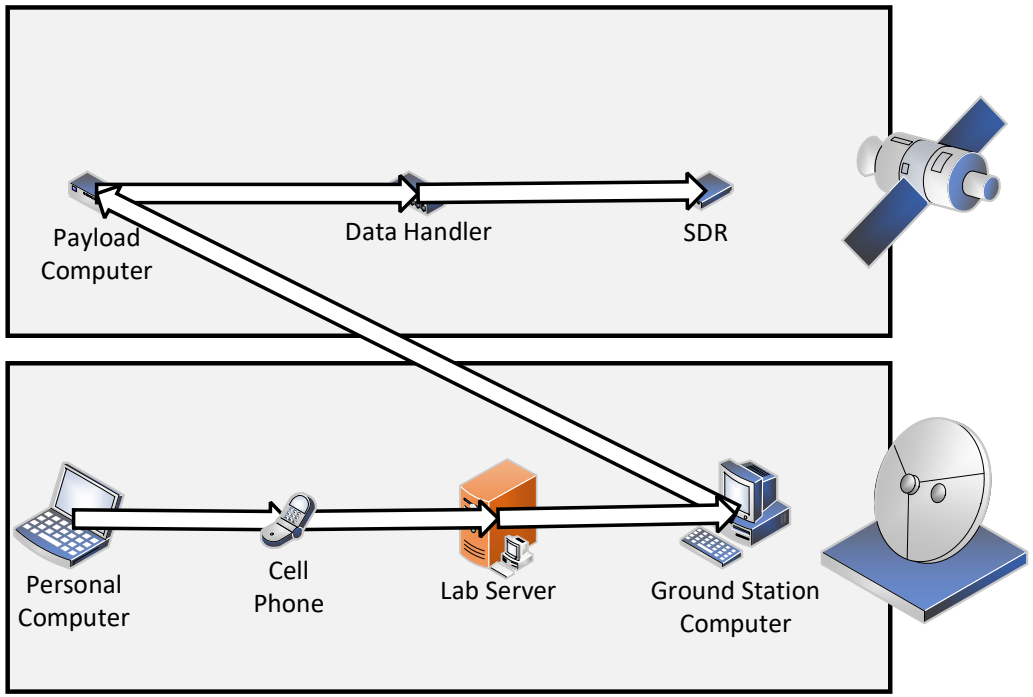








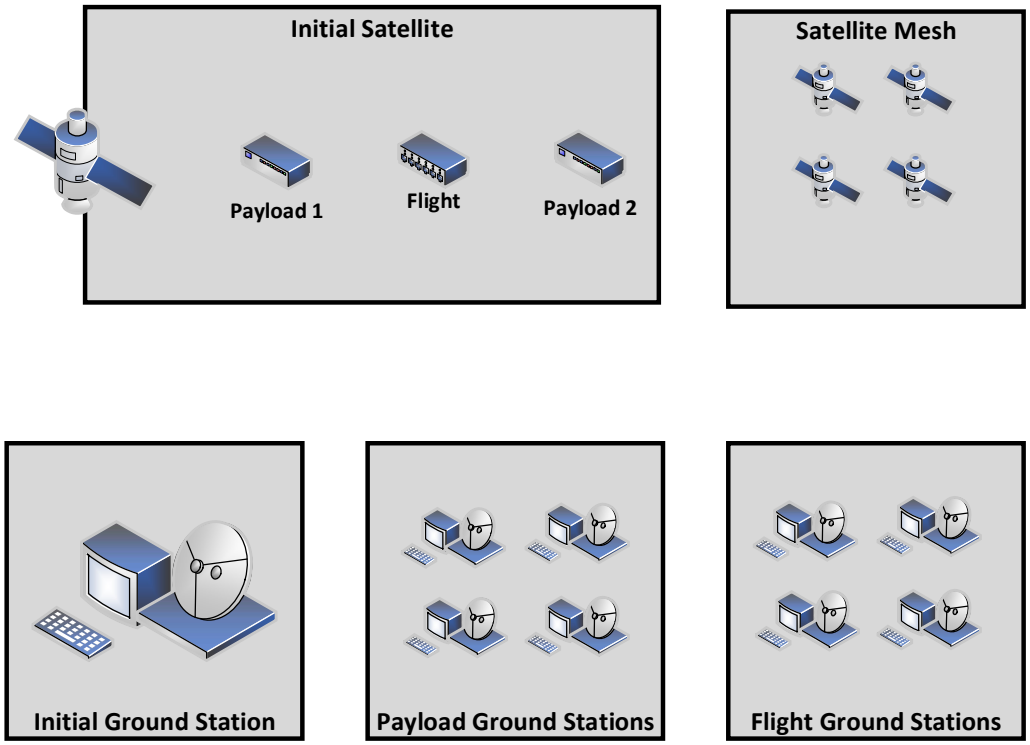


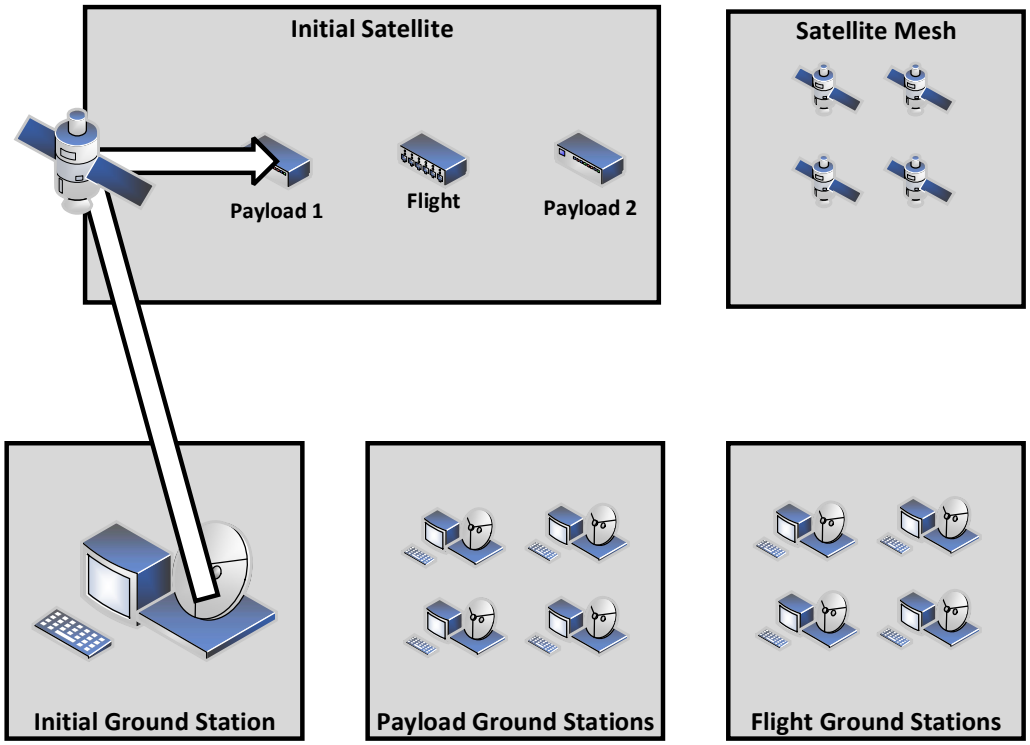


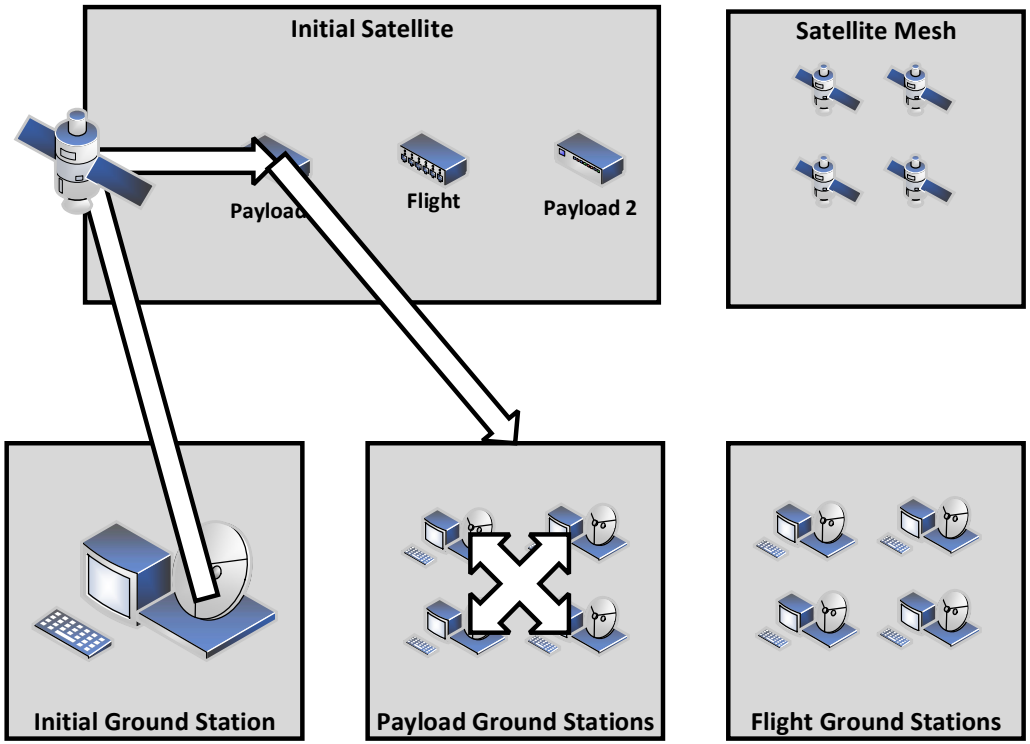
I wish it was that complicated…

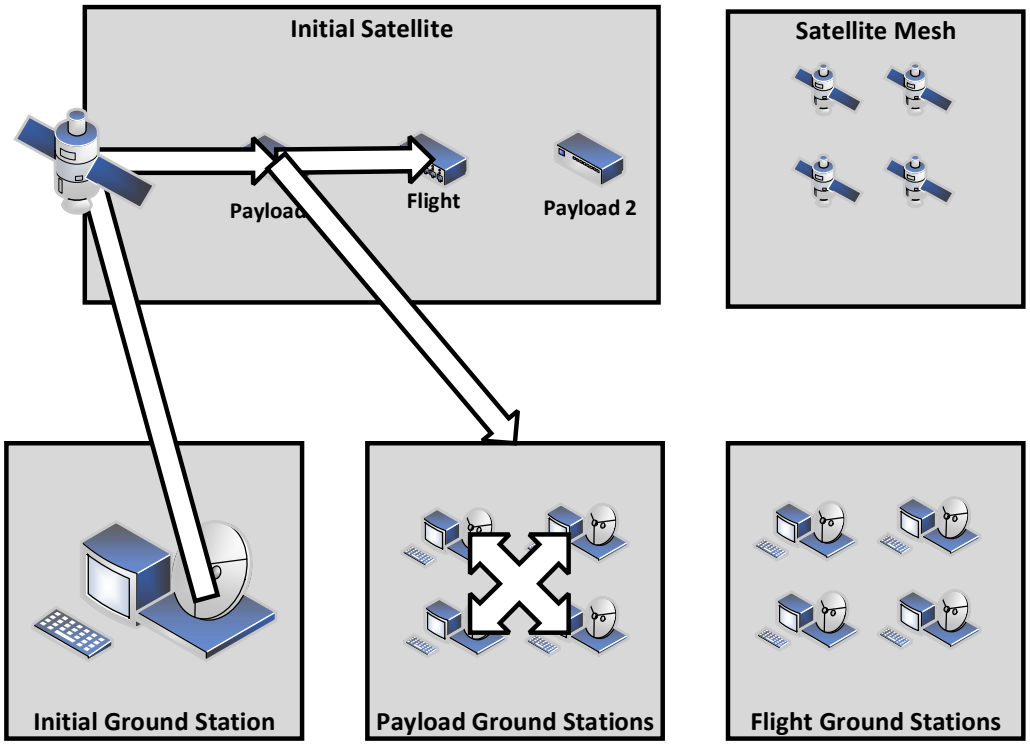
- Not being able to directly talk out to the internet does not mean air-gapped
- Things are connected to the internet that shouldn't be

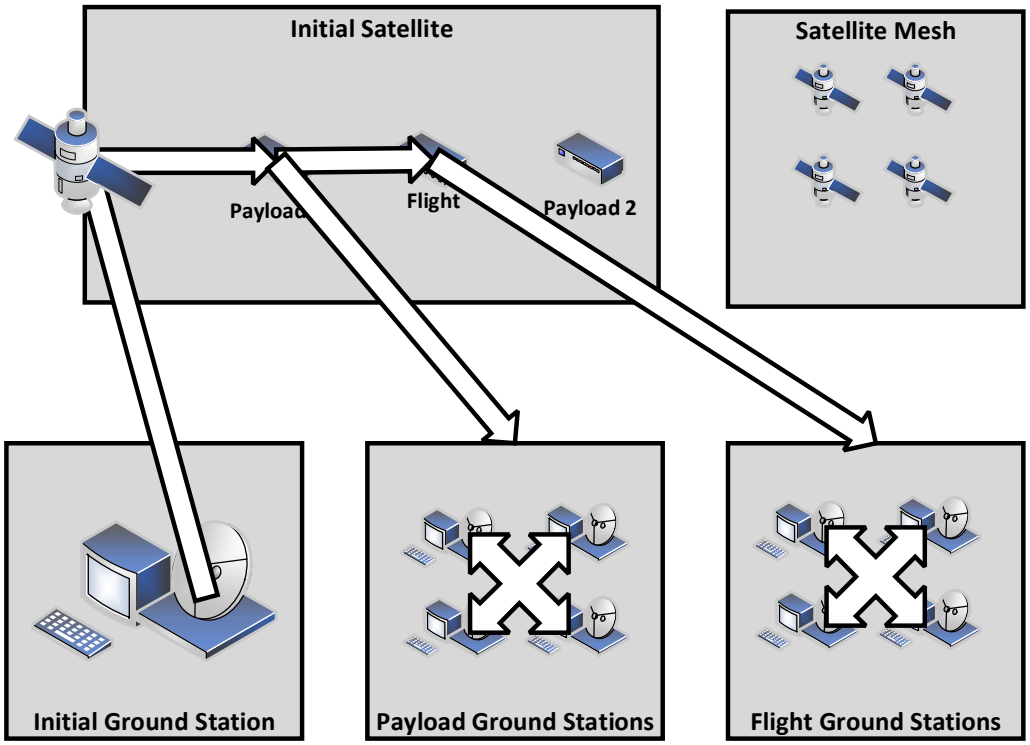
What about constellations?

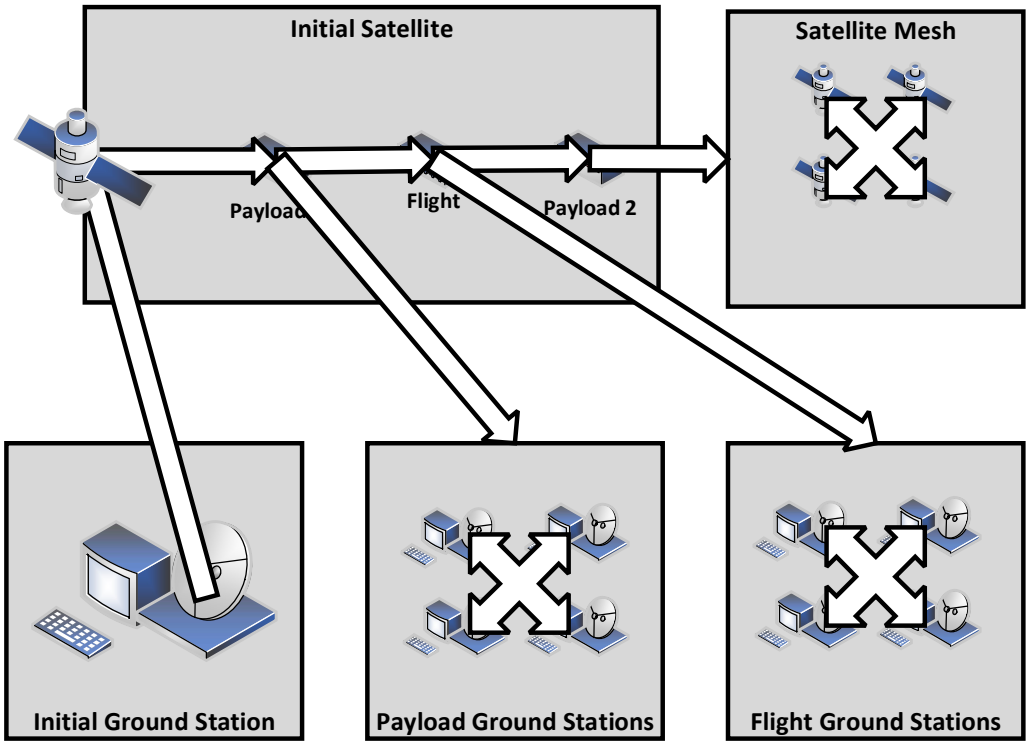












Who is Garak? He has a adversarial mindset!