

Commercial Antenna Security

Risks Real and Imagined with Using Commercial Antenna Systems on Critical Space Programs

Gerry Simon – Technical Director / Space Engineering Solutions / Parsons

© 2024 by Parsons Corporation, Published by The Aerospace Corporation with permission.

Proportionality Between Tools' Power and Tool Safety Risk

Moving Dirt Using Excavators


- **Reward:** 1/135 yds³ per shovel, 1 yds³ per typical excavator (68 yds³ max)
- **Risk:** 7 US Excavator Deaths in [2023](#)

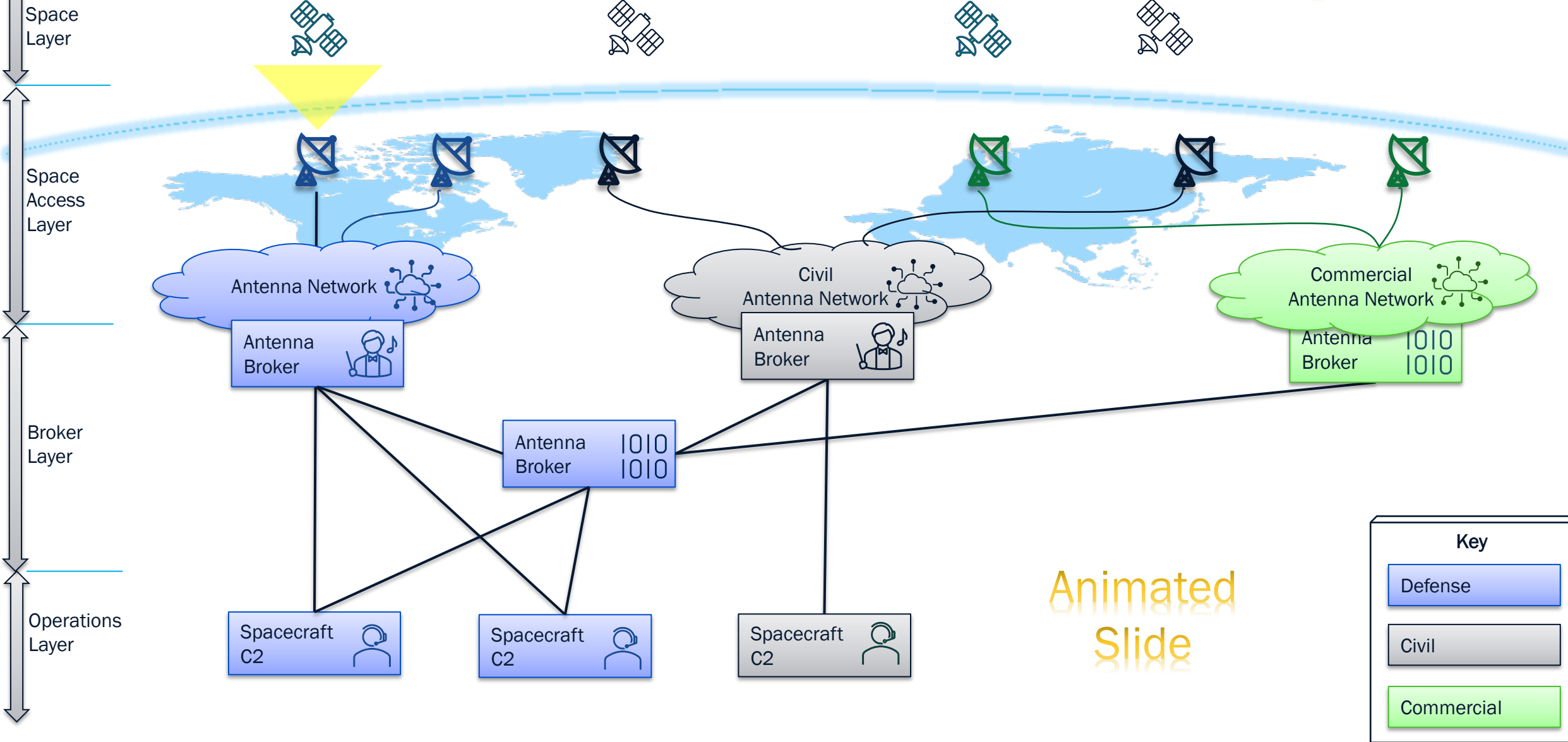


Flying Spacecraft Using Commercial Antennas

- **Reward:** Scalable to meet exponential growth in spacecraft
- **Risk:** ??

Spacecraft Access Evolution

 Space Based Access Point



Animated Slide

Key

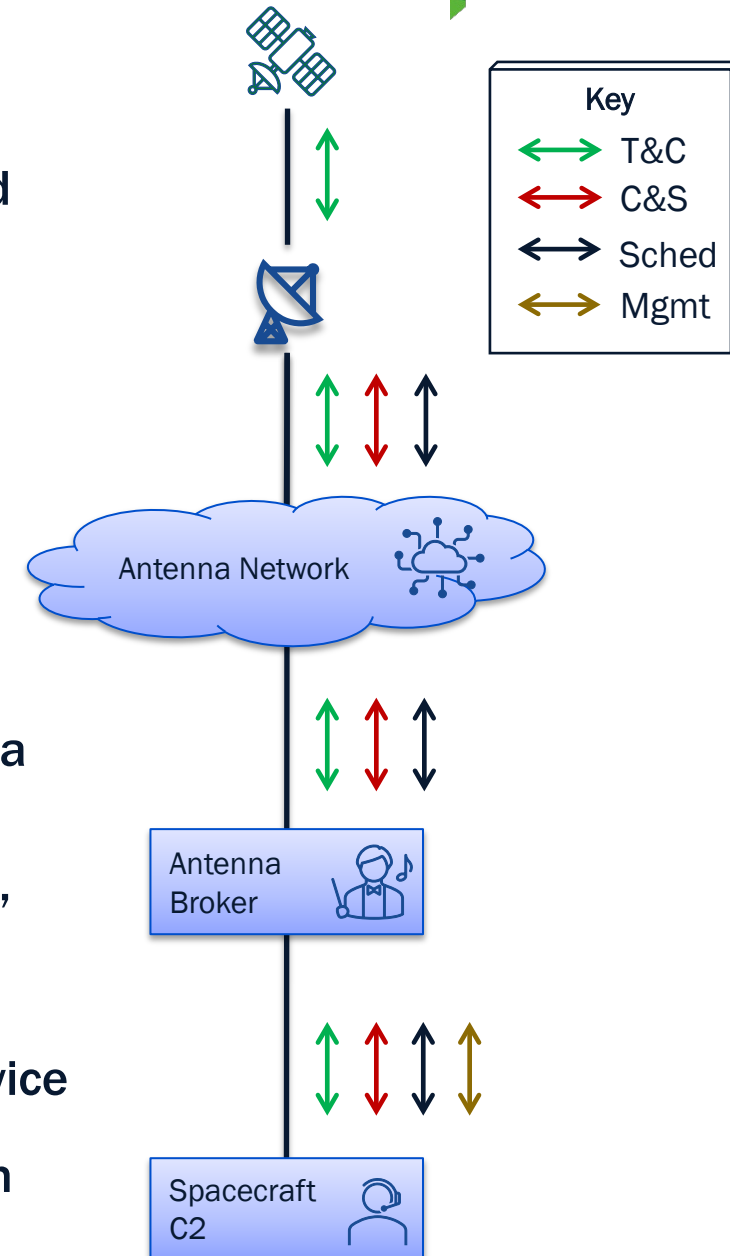
Defense

Civil

Commercial

Antenna Communications Planes

- **Data Plane (T&C):** contains the forward (command) link data and the return (telemetry) link data to and from a spacecraft. This data is typically end-to-end encrypted.
- **Control & Status Plane (C&S):** contains all the monitor and control data associated with controlling the Spacecraft Access Point (SAP)s. May include modem control and status, High Power Amplifier (HPA) control and status, antenna tracking angles, range, range rate, and/or status about the site itself such as weather.
- **Scheduling Plane (Sched):** contains all the information required to coordinate, and schedule contacts between SAPs and spacecraft. Scheduling is often an interactive process between multiple spacecraft operators and SAP owners which typically have multiple SAPs scheduled through their respective Antenna Broker(s). Schedule requests can become infinitely complex.
- **Provisioning Plane (Mgmt):** contains all the communication required to create, update, and delete new spacecraft with an antenna provider and/or broker. Similarly, the Provisioning Plane contains all the communication required to create, update, and delete new antennas with an antenna broker and/or Operator. This interface is part of the process involved with establishing a service relationship with an antenna provider and an antenna user; this process oftentimes involves contracts, licensing, payment arrangements, and NDAs. In the current state of practice, this interface is entirely manual and laborious.

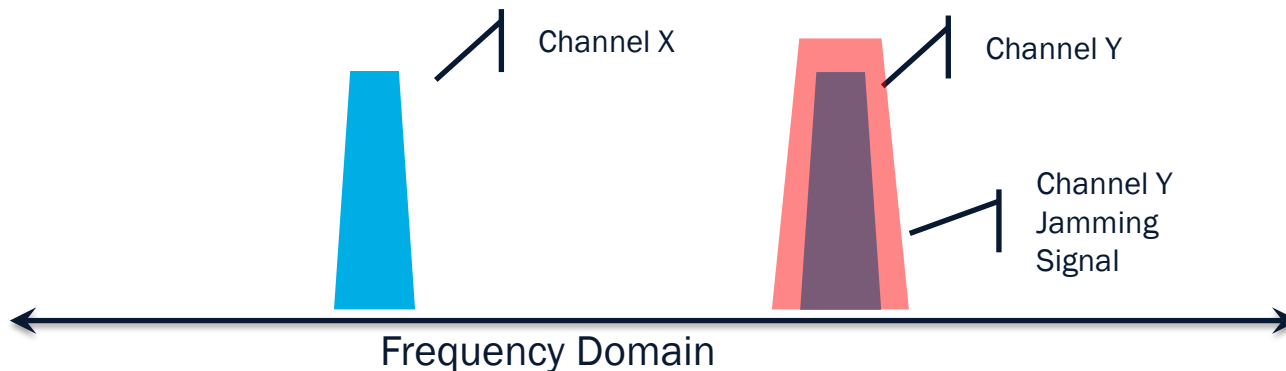
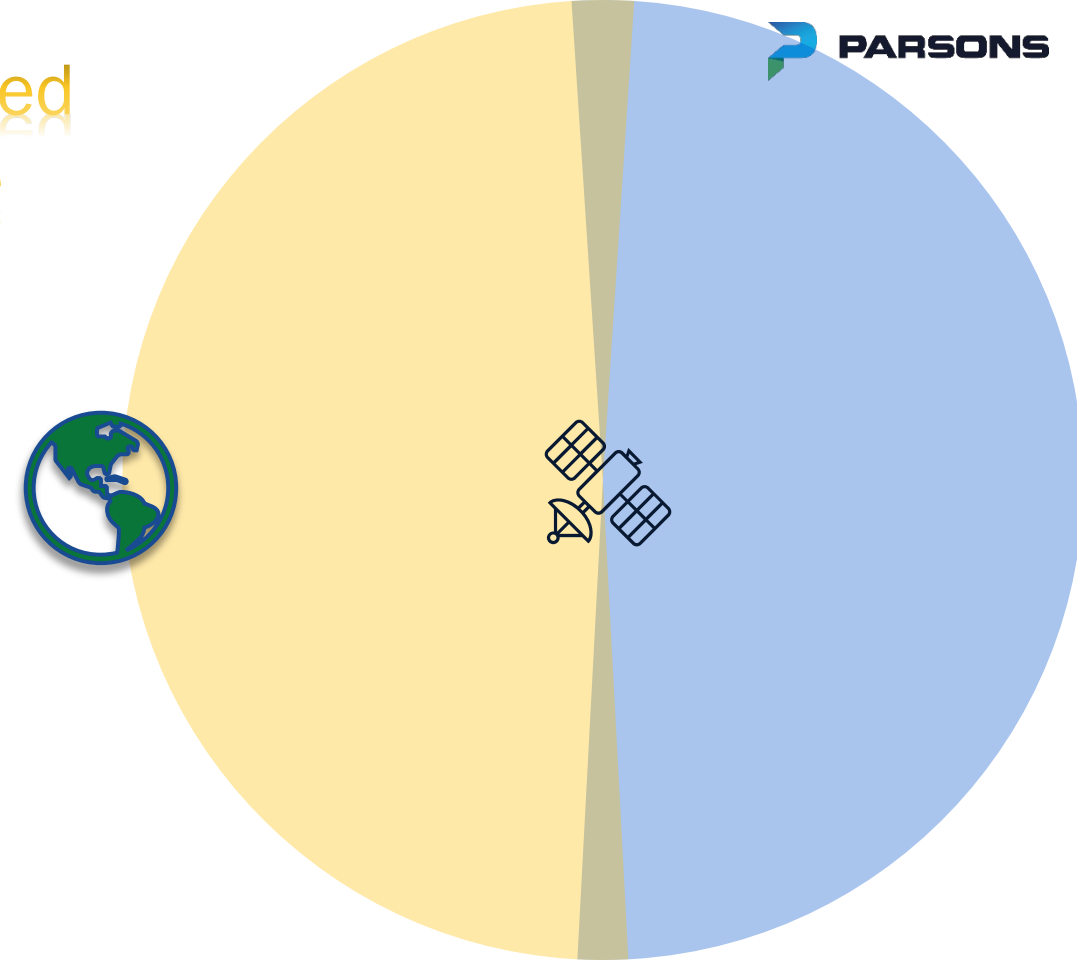


Physics of TT&C

• Omni T&C Antennas

- Spacecraft employ low gain, omni directional antennas for TT&C to ensure contact with the spacecraft regardless of the spacecraft/antenna orientation.
- Telemetry is broadcast everywhere the spacecraft is visible (easy to intercept).
- Low gain antennas means telemetry reaches the earth with low power.

Animated
Slide



• Channelized TT&C Signals

- Bright lines in a spectral graph (easy to detect)
- Jammable (both accidental and intentional)

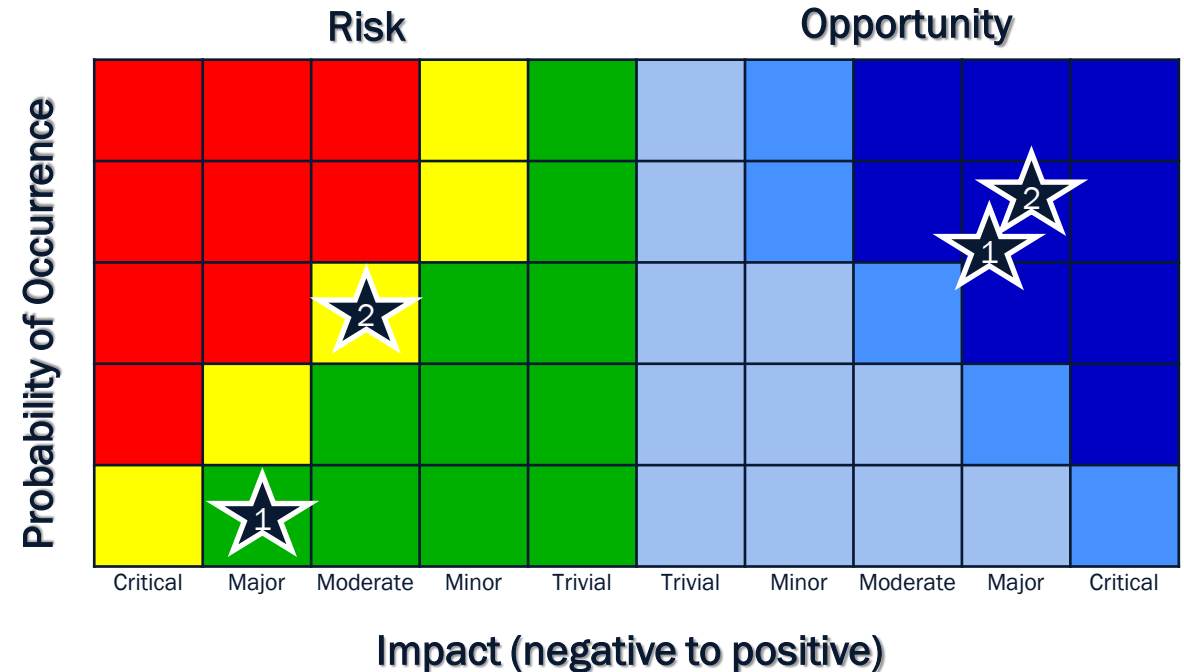
Risk & Opportunity Review (1 of 2)

1. Data Plane

- If an attacker gains control of a commercial T&C Plane, then they could intercept, deny or spoof either or both the command and telemetry data.
- Risk Assessment (P1, I4)
 - Probability is 1 because in almost all cases, the T&C data is fully encrypted, and spoofed T&C can be easily detected
- If a Spacecraft Operator seeks commercial antennas, then they could increase their access to space thereby increasing mission throughput, and resilience.
- Opportunity Assessment (P4, I4)

2. Control & Status Plane

- If an attacker gains control of the commercial C&S Plane, then they could deny access to the antenna or worse spoof radiometric data (e.g. tracking) coming from the spacecraft.
- Risk Assessment (P2, I3)
 - Probability is 2 because commercial providers limit C&S, access is protected via commercial authentication, and providers are financially incentivized to protect this.
- If a Spacecraft Operator seeks commercial antennas, then they could increase their access to space thereby increasing mission throughput, and resilience.
- Opportunity Assessment (P4, I3)



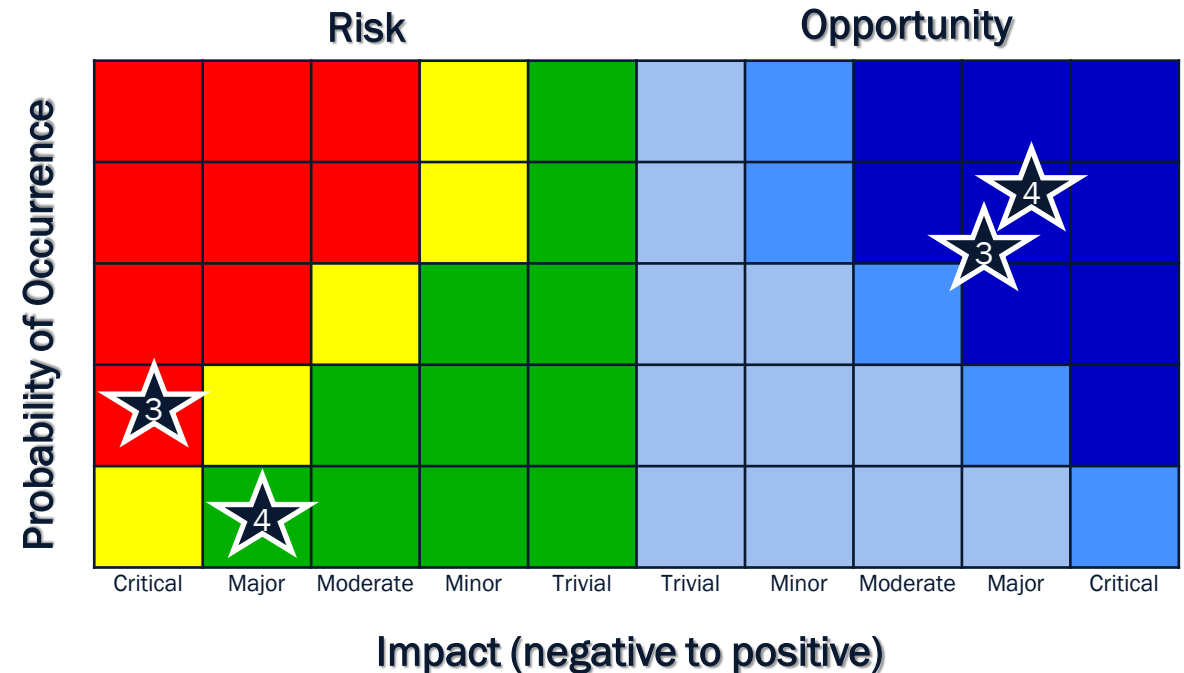
Risk & Opportunity Review (2 of 2)

1. Scheduling Plane

- If an attacker gains control of the commercial Scheduling Plane, **then** they could block access to antennas or grant access to antennas that aren't available, it would enable traffic analysis of critical missions.
- Risk Assessment (P2, I4)
 - Impact is 5 because advertising resources that aren't available could disrupt normal mission execution and could divulge heightened mission activity.
- If a Spacecraft Operator seeks commercial antennas, **then** they could increase their access to space thereby increasing mission throughput, and resilience.
- Opportunity Assessment (P4, I4)

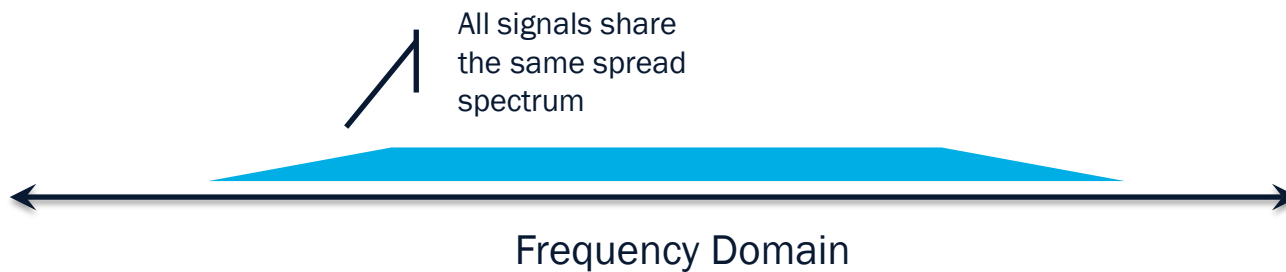
2. Management & Provisioning Plane

- If an attacker gains control of the commercial Provisioning Plane, **then** they could alter key configuration settings and disrupt operations from commercial antennas.
- Risk Assessment (P1, I4)
- If a Spacecraft Operator seeks commercial antennas, **then** they could increase their access to space thereby increasing mission throughput, and resilience.
- Opportunity Assessment (P4, I4)



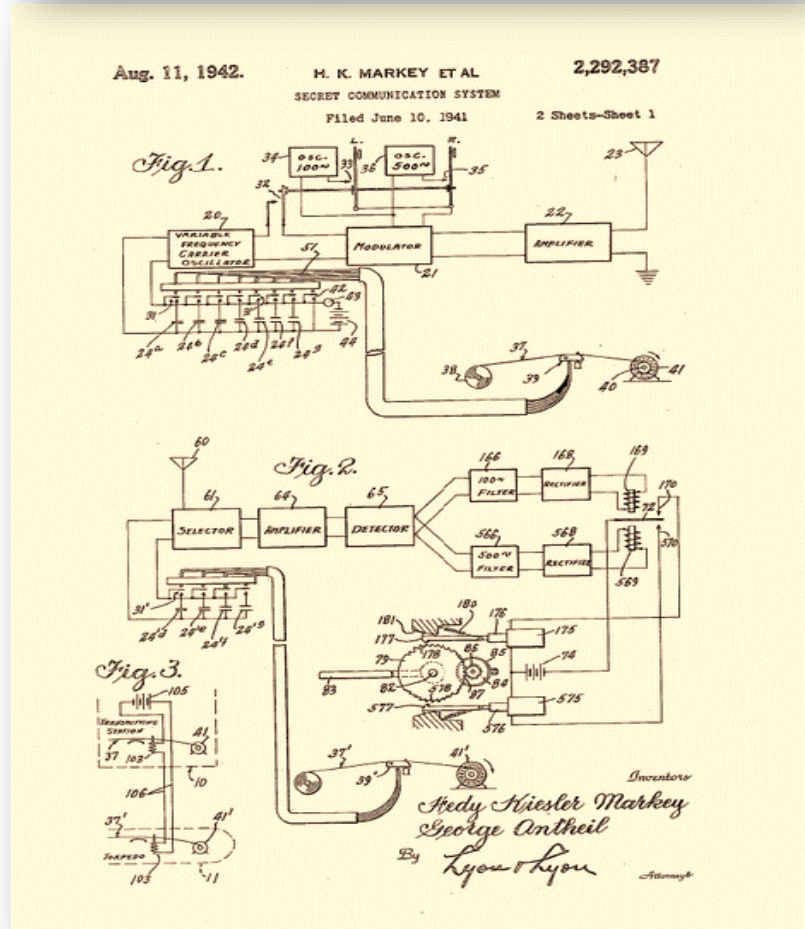
Recommendations & Mitigations (1 of 2)

- The single biggest risk driver is in the space to ground link which has nothing to do with whether the antennas are government or commercially provided. Mitigations are as follows:
 - Modernize TT&C Waveforms: specifically, to incorporate spread spectrum technology to make signals significantly harder to detect, intercept, jam.
 - Modernization should also include cognitive radios to more efficiently use bandwidth and enable resilient real-time waveform alterations.
 - Don't depend on all commercial (and government) antenna systems to accommodate waveform modernizations - move the Radio back to the control center by using IF or RF Over IP.



Bonus: RFI Mitigation is at the same level of cell phones!

Hedy Lamar patented spread spectrum in 1942



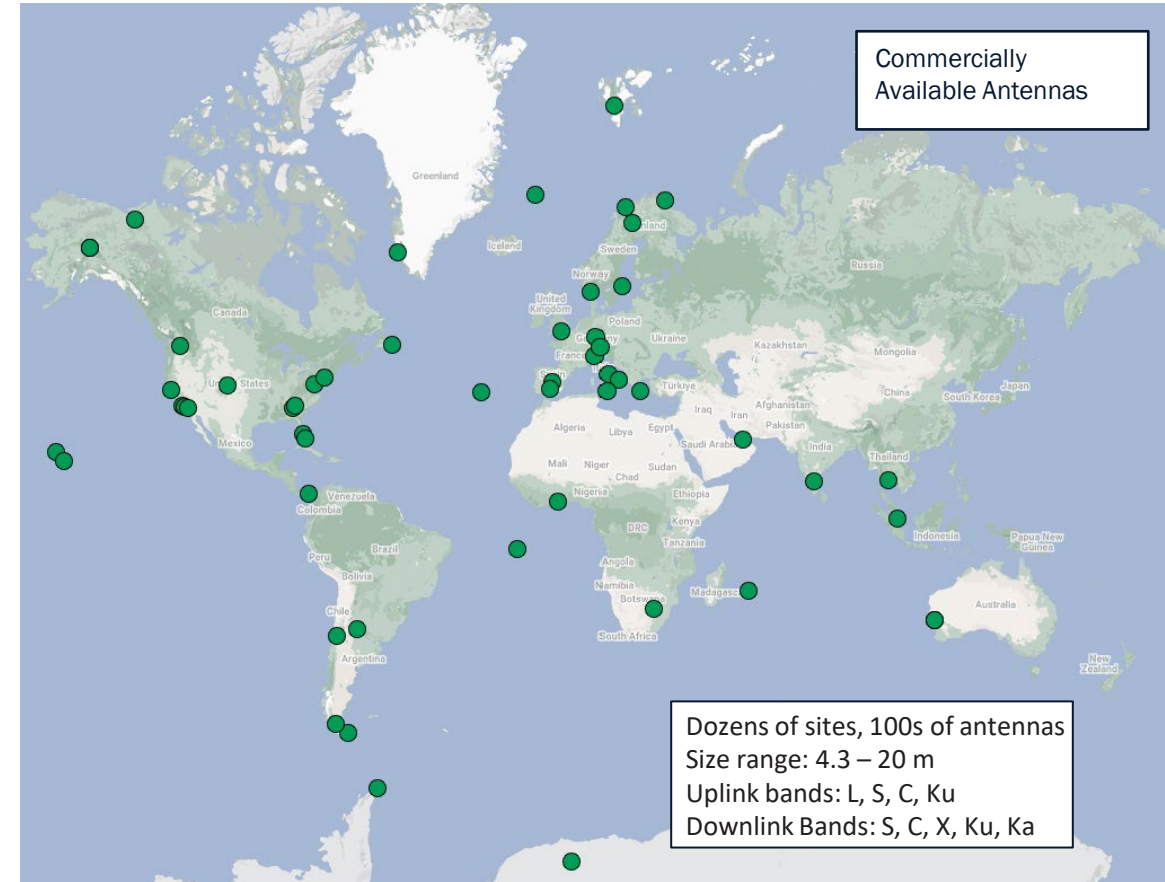
Recommendations & Mitigations (1 of 2)

- **To Reduce the Risks stemming from exposing traffic to commercial providers:**
 - Obfuscate All Critical Space Assets by pre-brokering government spacecraft to commercial providers.
 - Additional obfuscation of Space Traffic is possible by running fake supports.

- **To reduce the risks associated with provisioning (vehicle specific configurations):**
 - Implement stateless control – all configuration done by the Spacecraft Operator.
 - Foster Greater Standardization for the Data, Control & Status, Scheduling and Provisioning planes with open interface standards.

- **In increase the opportunity of using anyone’s antennas:**
 - Support the development and incorporation of industry standards at every interface plane

- **Incorporate Every Ground Asset Possible**



Embrace Competitive and Commercially Provided Access to Space!



THANK YOU!