FINAL FRONTIER SECURITY

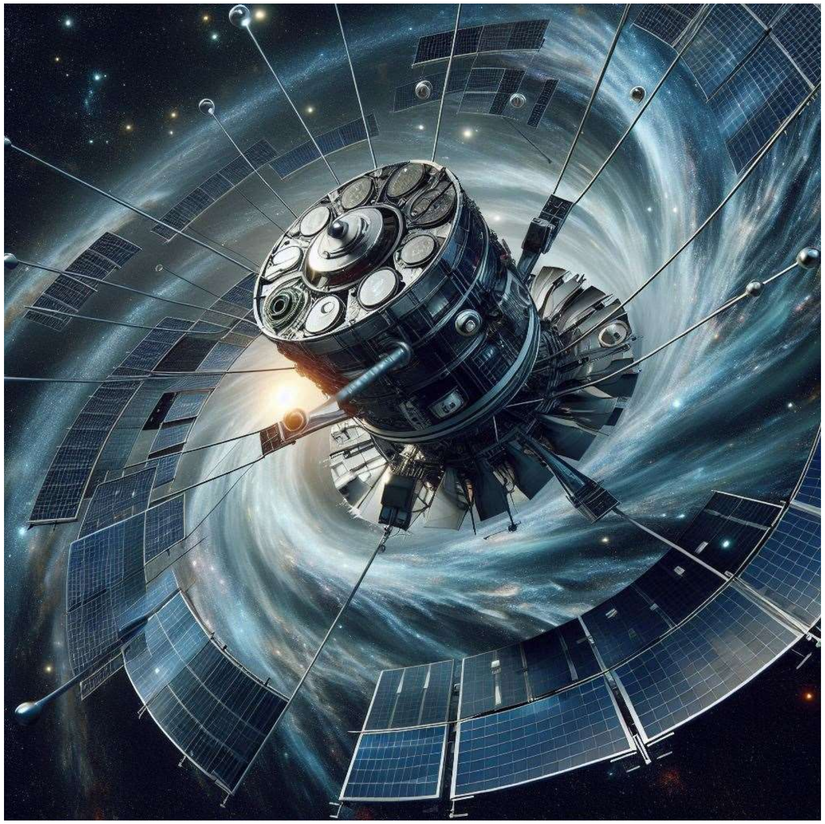
Lecture Three

The intersection of space and cyber

Class Day 2

- 0900 - 0945 Lecture 3: 45m Recap, Intersection of Space and Cyber
- 0945 – 1030 Lab 5: 45m Command Interceptor
- 1030 Break: 15m
- 1045 – 1115 Lecture 4: 30m The Future
- 1115 – 1215 Lab 6: 1hr cloaking device
- 1230 – 1345 Lunch
- 1400 – 1445 Lecture 5: 45m SPARTA
- 1445 – 11545 Lab 7: 1hr : Code Execution
- 1600 - Break: 15m
- 1615 – 1645: Lecture 6: 30m State of things
- 1645 - 1800 FFA lab time: 75m Go ahead and break it all, we will re-deploy tomorrow!

Recapping Yesterday’s labs



- Spinning a satellite around
- Real speed of movement vs what you saw in 42
- Slew rate, what it means and why
- Slewing while pointing at ground for communications
- Slewing while pointed at space to observe same target
  - JWST ~ 3 degrees per minute (this is slow)
- Slewing to observe a weapon
- Slewing implications
  - Antenna sheer
  - Loss of control
  - Damage to attitude control (actuators, fly wheels etc)

Recapping Yesterday's labs: Comms, DoS encryption etc

- So if I can point my antenna at a satellite and talk to it….?
- You would have to know the frequency and other RF related details to close the link
- You would have to know the radio salutation context
  - This prevents DoS
  - This prevents battery taxing
- You would have to have the encryption if it exists
- You would have to know the way the satellite takes tasks (packet construction / where file monitoring looks for things

PROBLEMS
PROBLEMS EVERYWHERE
imgflip.com

The Cost Problem

- Lack of cost metric for cybersecurity in general
- Obsession with flight heritage
- Can’t make informed risk acceptance decisions
  - Will default to risk acceptance (plenty of flight heritage for accepting risk, for cyber not so much)
- Mesh complications
  - Cost communication becomes more convoluted
  - Fixes and attacks can proliferate faster

The Culture Problem

- The Hayabusa story
- Usually, cybersecurity people are the most risk averse
- Normally cybersecurity people are the more technical people in the cybersecurity discussion
- The space industry is obsessed with risk
- The technical perspectives of people in the industry can complicate telling the cybersecurity story

Supply Chain Problem(s)

- Few proven vendors for buses, antennas, FPGAs and other significant components
  - Exceptional targetability for interdiction
- High probability of widespread industry disruption if a vendor has an issue
- Few proven launch providers
- The threat of time
  - Launch windows
  - Long lead parts

Disparity Problem(s)

- Space Rated Cyber: Disparity in Defense Vs Offense
- Even if resources, capabilities and numbers were the same:
  - Defensive capabilities must be space rated
  - System owners will see defensive tools as a threat to their mission
  - Defensive tools must fail open (lest they be weaponized)
- Specialization and limited supply chain and vendors allow attackers to hyper-focus on specific attack surface
- Lack of defense in depth

3rd Party Attack Surface Problem

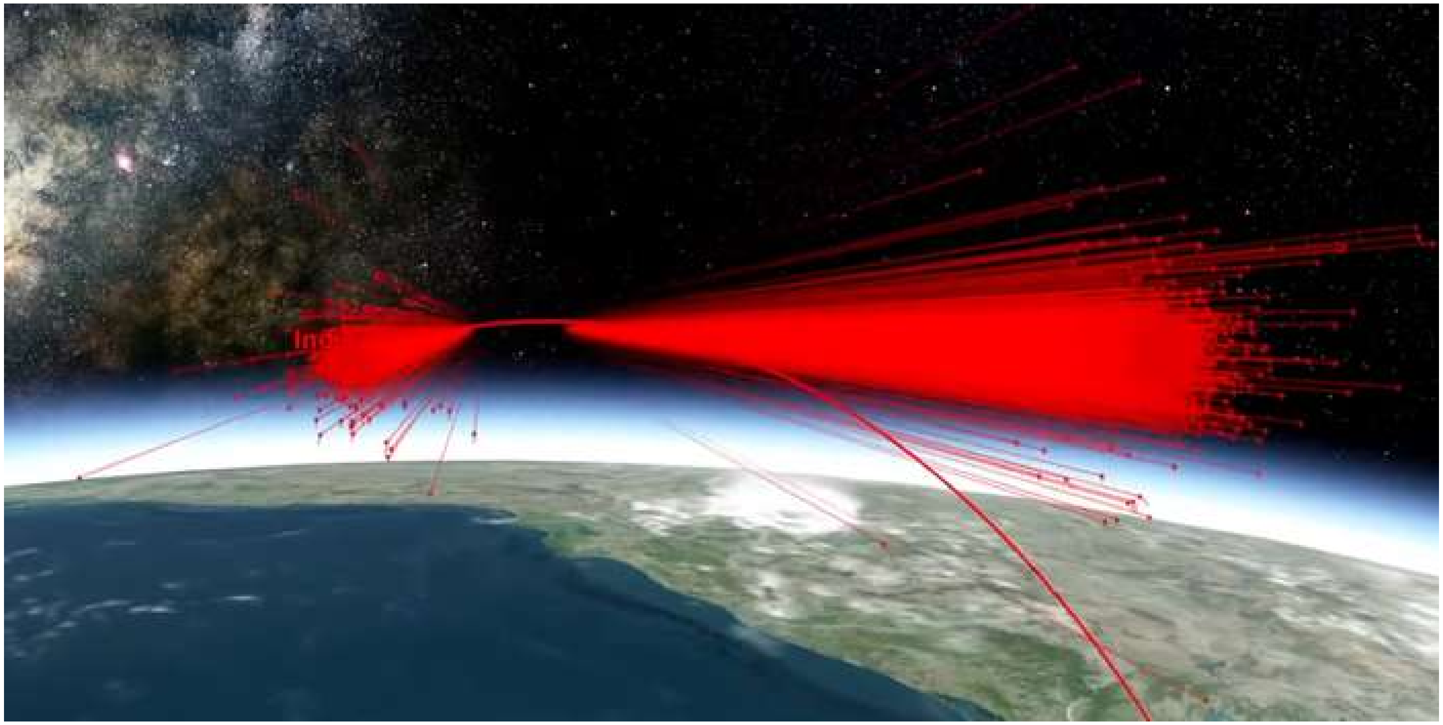
- Beyond SV resident code execution, an ability to impact a space system stretches far beyond the control of owners and operators
- Widely varied, targetable environmental testing facilities
  - Vacuum chambers
  - Anechoic chambers
  - Vibration tables, etc.
- Storage and transport for tests and launch
- Downstream services like analysis
- Customers

The Cyber Warfare Problem

- Suitability

Kinetic Anti-Satellite Weapons

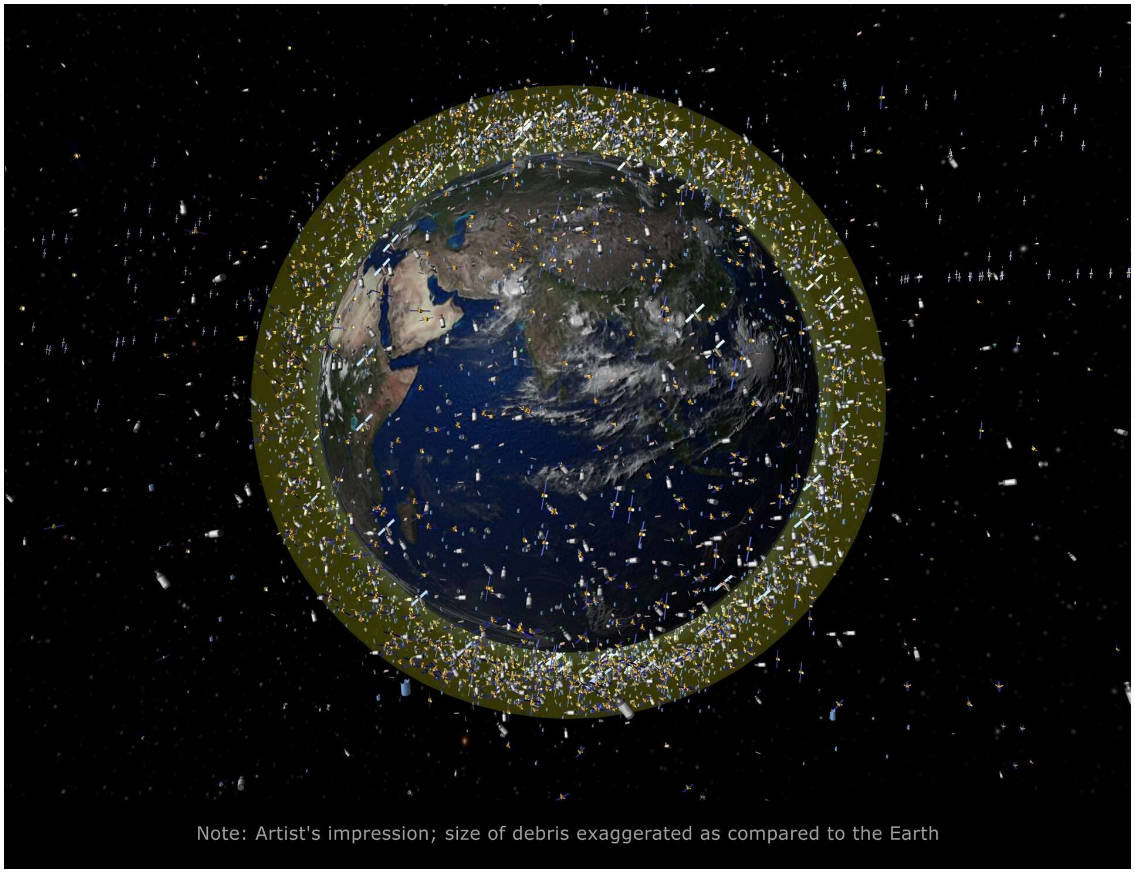
- Mission Shakti, Indian anti-satellite test
- 1600 lb. satellite turned into 6500+ pieces of shrapnel going 22,000 MPH+
- Debris field 175 miles above earth



A simulation of space debris created by India's "Mission Shakti" anti-satellite missile test on March 27, 2019. Analytical Graphics Inc.

Kessler Effect

- One event could cascade into more, polluting entire orbital areas
- SpaceX alone at 5,000+ already
- Launches accelerating
- More space objects = worse curve for Kessler Effect


Note: Artist's impression; size of debris exaggerated as compared to the Earth

The Test & Evaluation Problem

- RMF and IV&V is validation and evaluation not exercise of security apparatus

- All other tests for space systems exercise

- Torque bolt measurement vibe test analogy

The Adaptation Problem

- All non-cyber challenges are solvable and can be evaluated / exercised in repeatable defensible manners

- Cyber threat is constantly undermining preventative measures and extremely difficult to defensibly evaluate implementations.

The Defense In Depth Problem

- Components and systems are too trusting

- Communications within space system too trusted (all encrypted so everything is fine right?)
  - Ground to vehicle
  - Vehicle to vehicle
  - Vehicle to ground

- Computationally intensive defenses end at ground station, if present there at all

The Modernization Problem

- Transition to more common OS for portability and resources must be done correctly

- Not just for developmental and integration ease but also leverage that technology’s security features

- Other wise attack surface is worse off going from a one off unknown old piece of software to a well understood and unsecure modern one

The Failure Analysis Problem

- Software definition of space system functions will continue

- Anomaly or failure on a space vehicle might have been intentionally caused by a cyber effect needs

- Cyber attacks need to be explored as a cause during failure analysis in tandem with or in high priority amongst other potential root causes

The Disclosure Problem

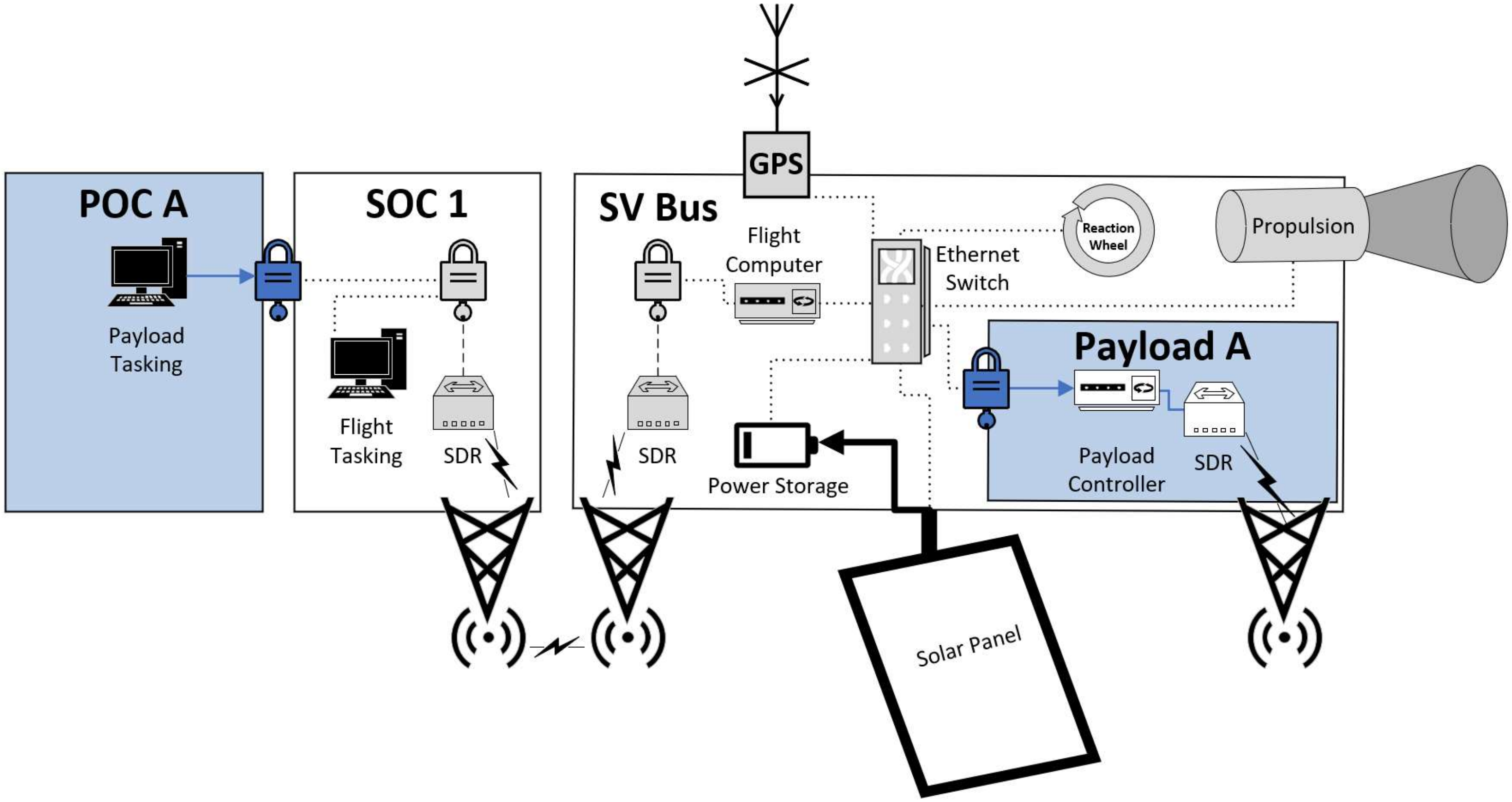
- Most of these systems are owned or utilized by governments and militaries who are not required to, or have it in their best interest, to disclose compromises or vulnerabilities

- This impacts the ability to do effective heuristic detection with large sample sets, giving a leg up to the adversary

Electronic Warfare

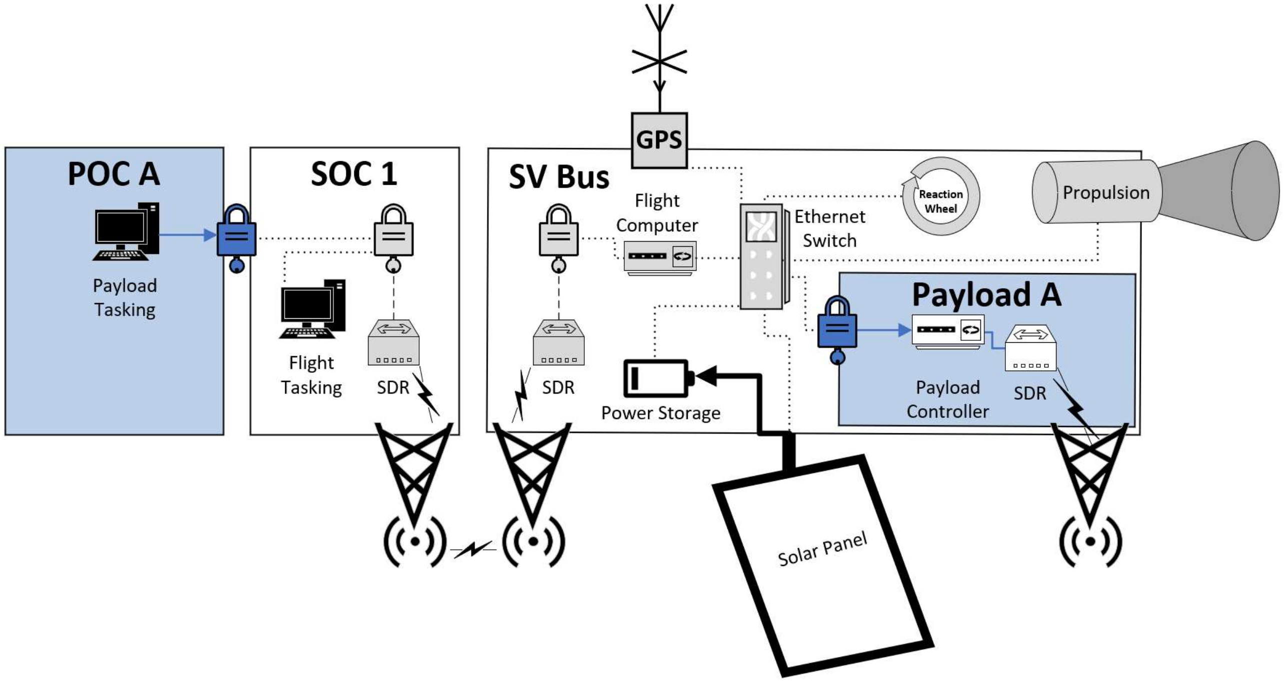
- Jamming
- Spoofing
- Importance of separating from cyber threats
- Is this cyber? Is this a cybersecurity problem?
- Why is it problematic to too closely associate the two
  - From a defensive perspective
  - From an offensive perspective

Organic Attack Surface



2nd Party Attack Surface

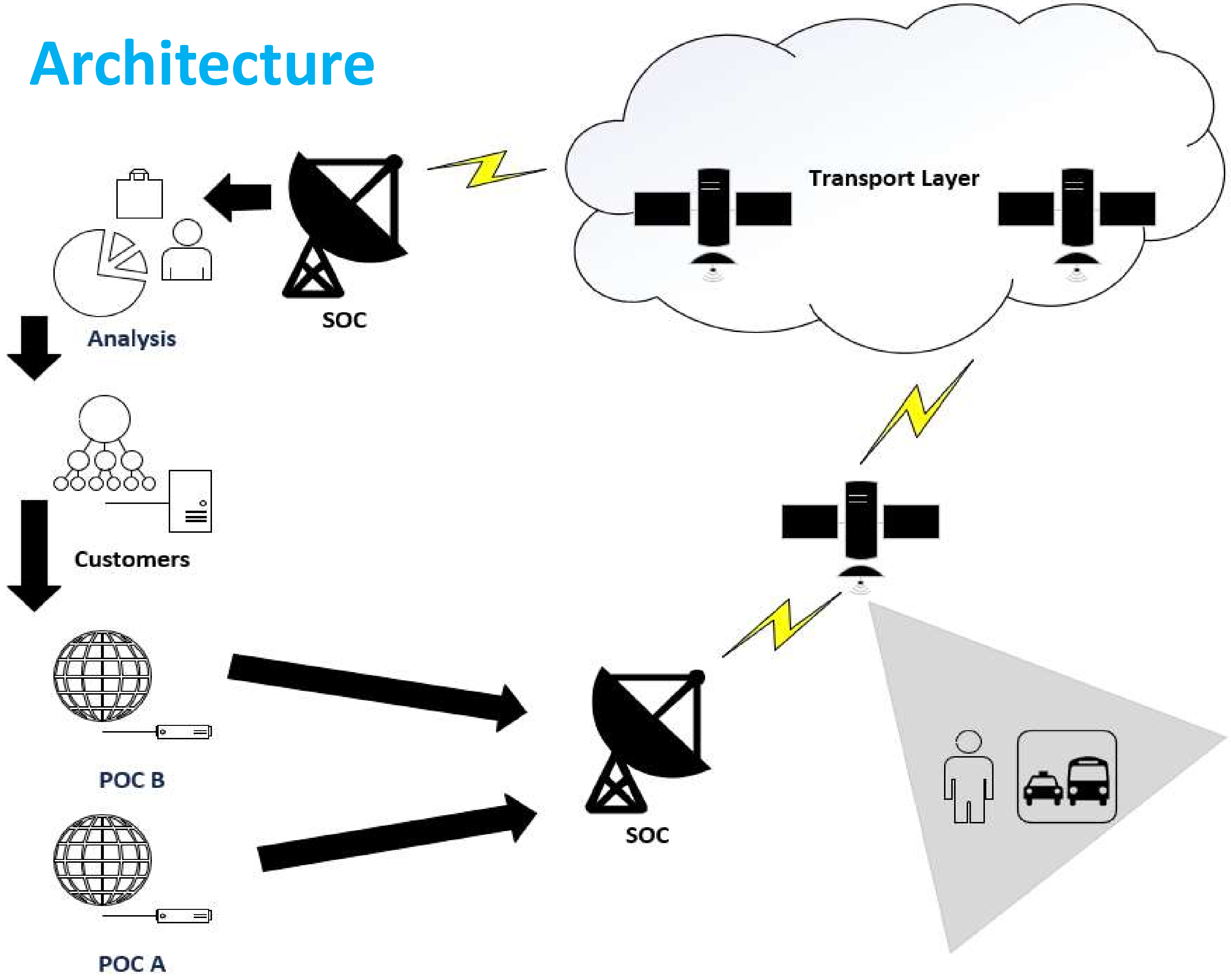
- Hosted Payloads scenario
  - Satellite Operator(s)
  - Payload Operator(s)

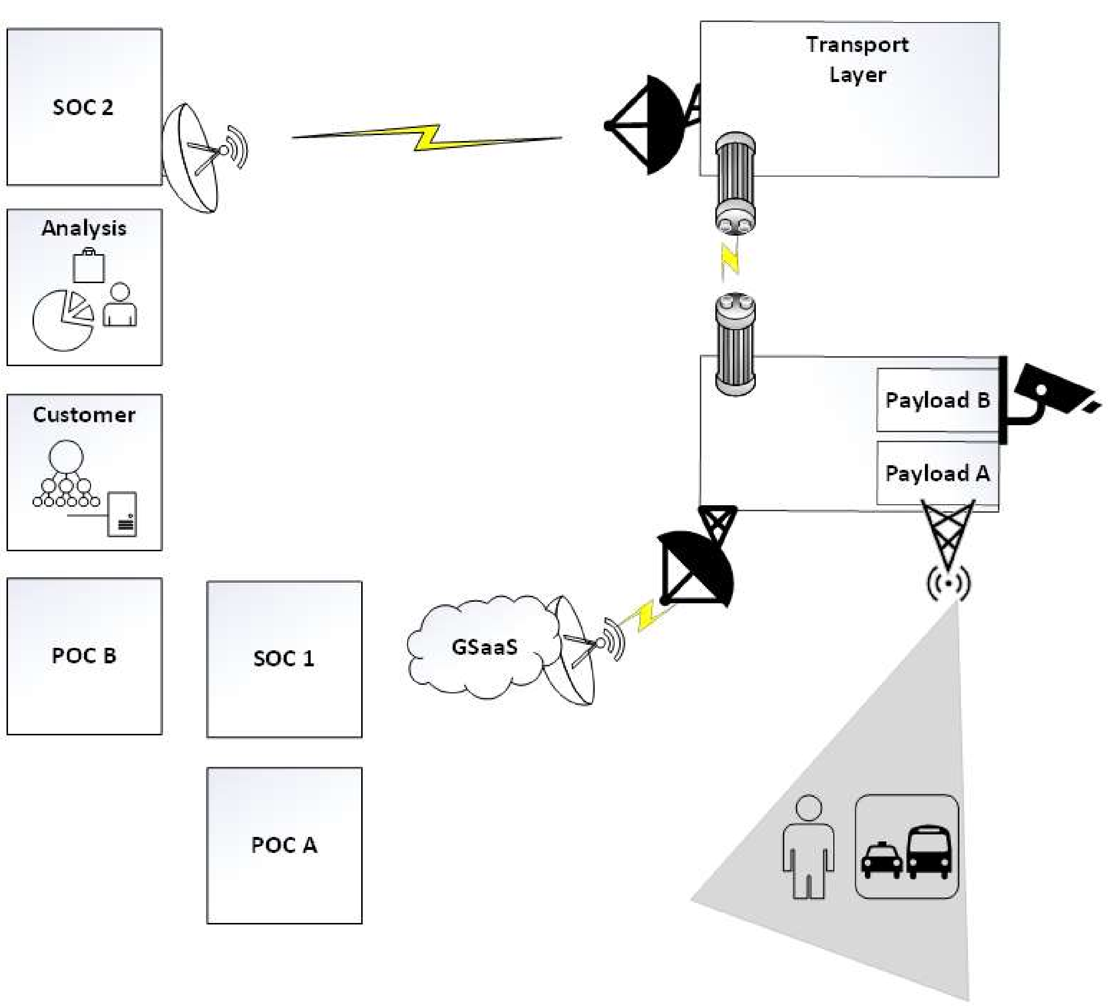


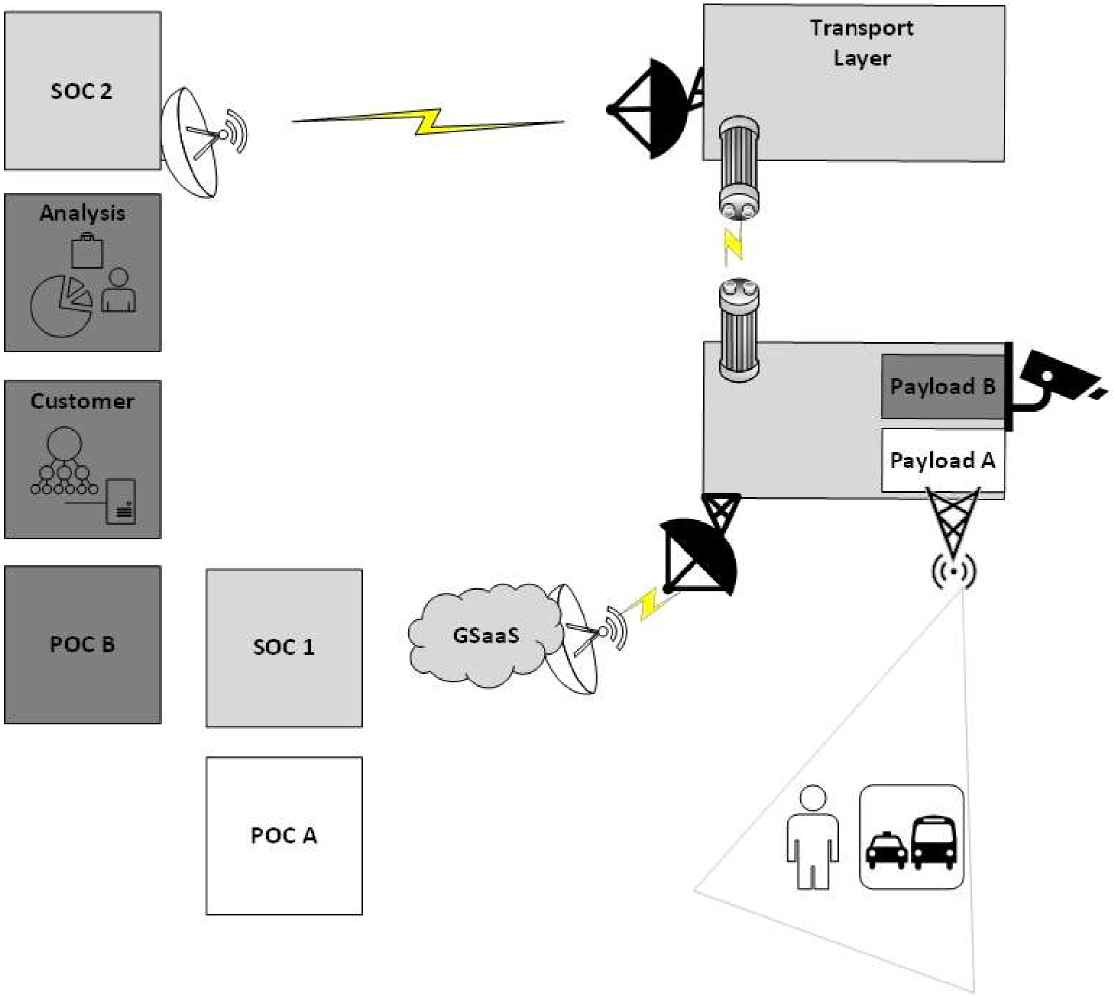
3^{rd} Party Attack Surface

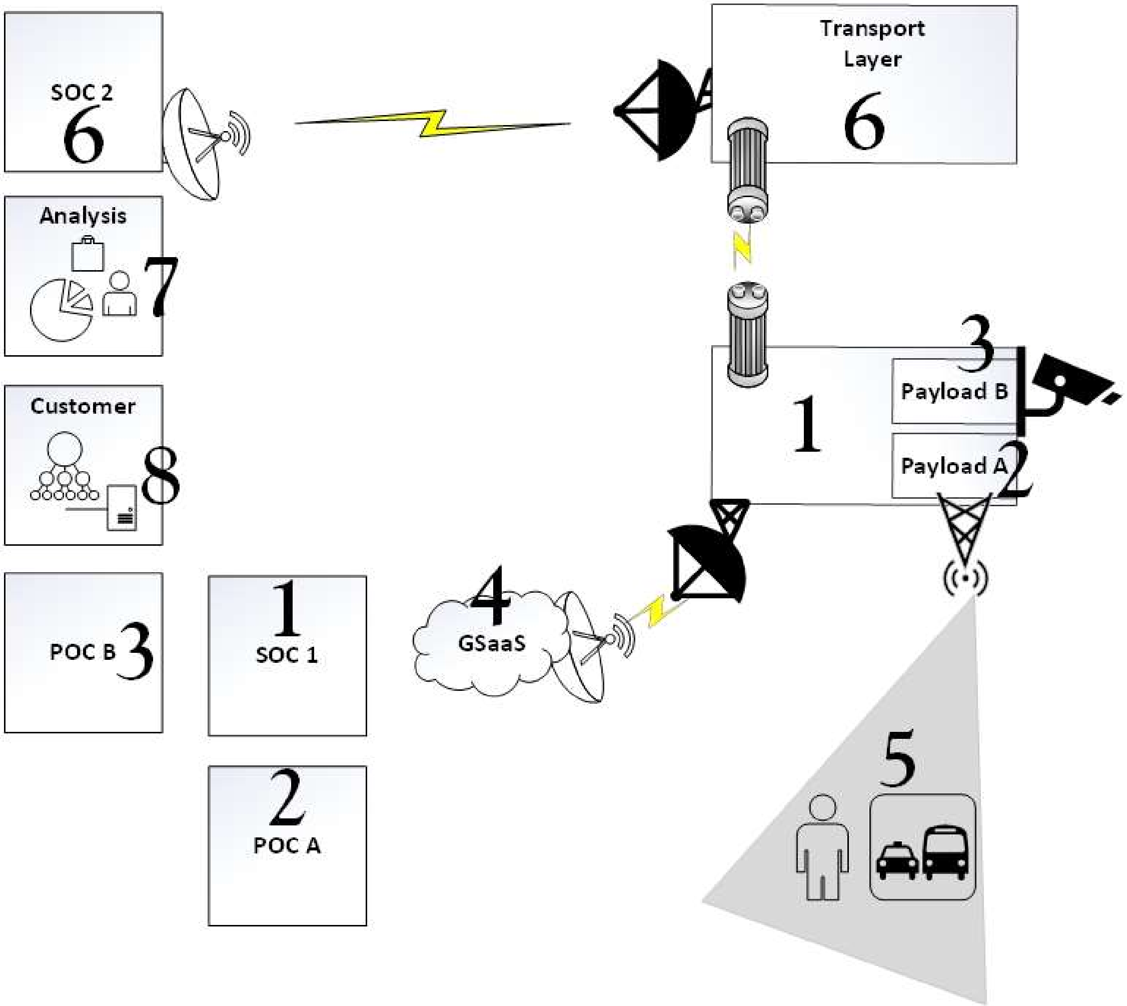
- Beyond SV resident code execution, an ability to impact a space system stretches far beyond the control of owners and operators
- Widely varied, targetable environmental testing facilities
  - Vacuum chambers
  - Anechoic chambers
  - Vibration tables, etc.
- Storage and transport for tests and launch
- Intra-vehicle tenants & operators

Architecture

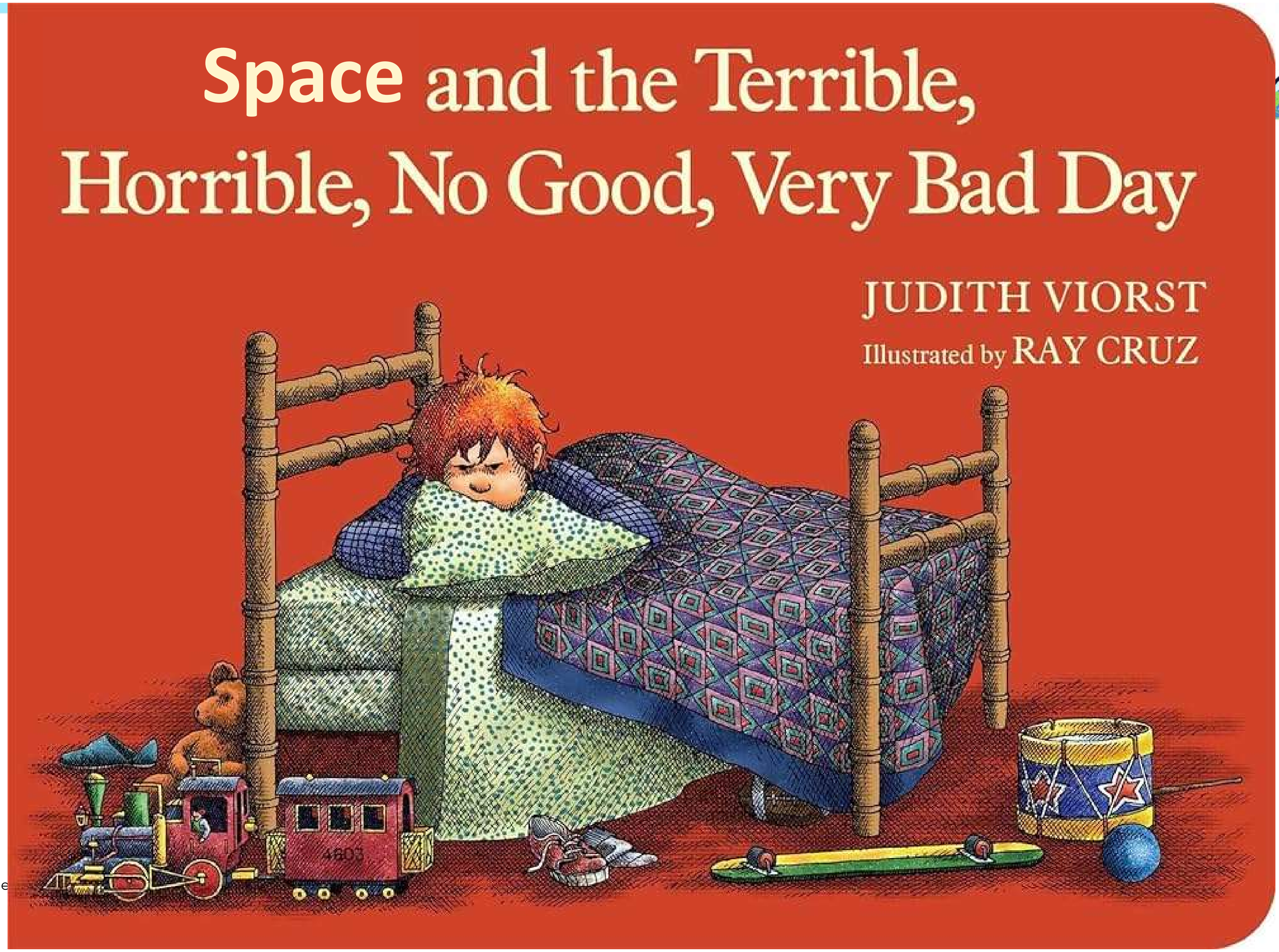



SOC 2
Analysis
Customer
POC B
SOC 1
POC A
GSaaS
Transport Layer
Payload B
Payload A


SOC 2
Transport Layer
Analysis
Customer
Payload B
Payload A
POC B
SOC 1
GSaaS
POC A



1. SOC 1 and the satellite Bus are owned by a company offering payload hosting.
2. POC A and Payload A are owned by a broadcast radio company
3. POC B and Payload B are owned by a imaging company that takes sensitive images as a service
4. GSaaS provided by a 3rd party commercial organization.
5. Users of satellite radio are another customer.
6. The transport layer SOC 2 and its satellites are owned by a different commercial organization.
7. Analysis of the images is a different organization.

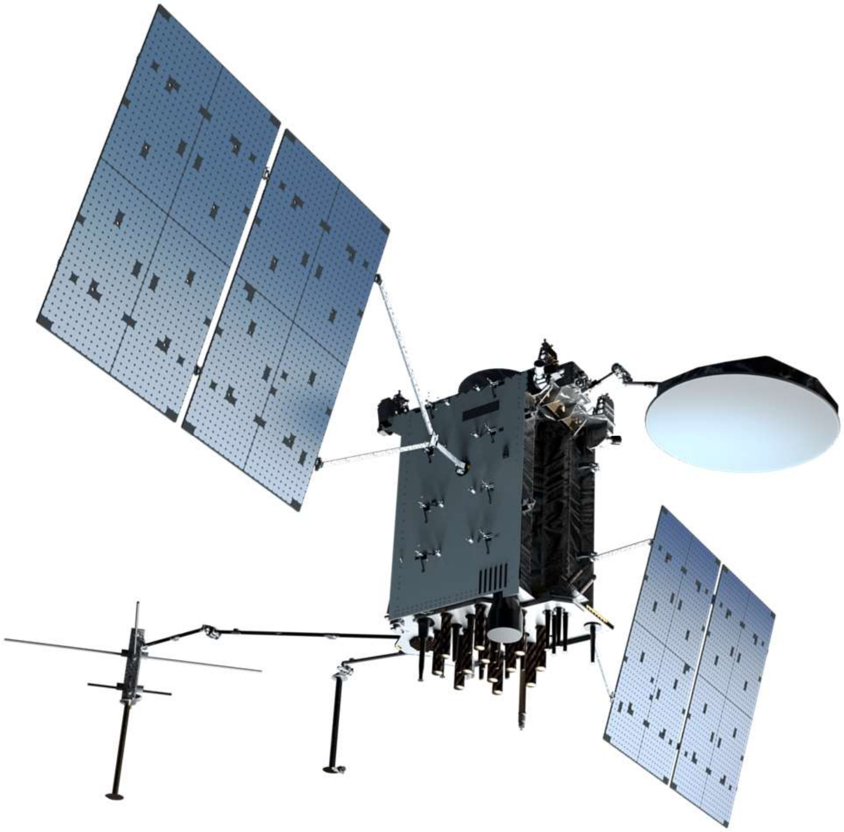

Space and the Terrible,
Horrible, No Good, Very Bad Day
JUDITH VIORST
Illustrated by RAY CRUZ
4603

Scary Story Time

- You stole the satellite(s)?
- Admittedly (hopefully) oversimplified example:
  - Task an update to the satellite(s) that replaces encryption keys
  - Start talking to your new satellite from your own ground station(s)
- But....that's not realistic right?.......Right?

Money Talks (and so does national security)

- Single Lockheed Martin GPS 3F satellite ~$250M
  - https://spacenews.com/u-s-space-force-buys-three-new-gps-satellites-from-lockheed-martin/
- GPS constellation: Lockheed Martin is now producing a more advanced version, the GPS 3F. The company in 2018 was awarded a contract worth $7.2 billion for up to 22 GPS 3F satellites.
  - https://spacenews.com/air-force-to-award-7-2-billion-contract-to-lockheed-martin-for-22-gps-satellites/
- GPS over time: “Reports estimate that since the 1980s, GPS satellites have helped generate nearly $1.4 trillion in economic benefits”
  - https://aerospace.org/article/brief-history-gps

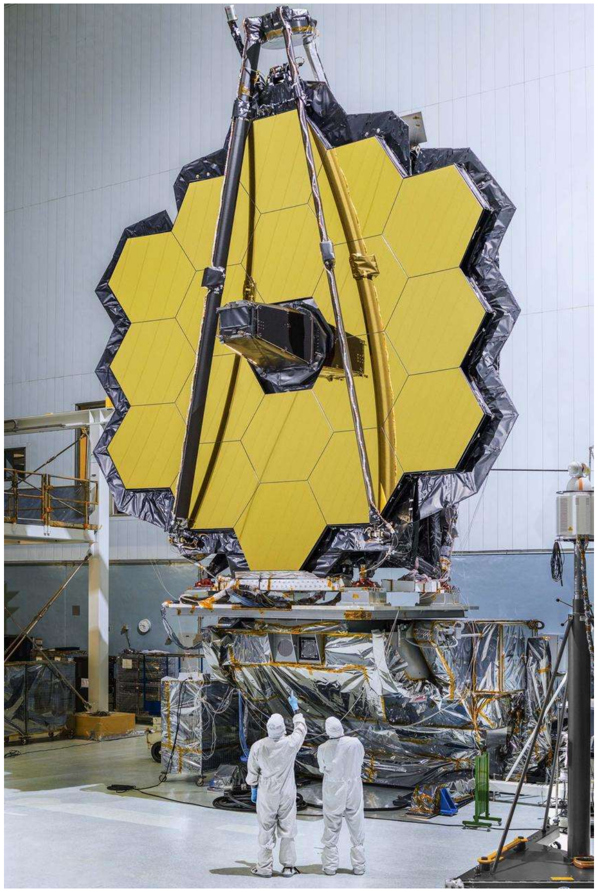


Let’s run some numbers

- 2023: US servicemember with clearance passes detailed classified technical manuals and documents to foreign Intelligence for $5,000.
- 2024: US servicemember with clearance enters restricted compounds to take information and pass along to foreign intelligence for $15,000
- 2024: US servicemember with top secret clearance downloads and sells to foreign intelligence for $42,000
- What do we think a foreign government would be willing to pay to instantly own the GPS constellation? A million? Ten million? A billion?
- Also, we’d then just shoot them down, right? No. Remember, you’d pollute the orbit with hypersonic shrapnel.

Not convinced? How about a softer target?

- James Webb Space Telescope (JWST)
- Cost: $10 Billion
- https://www.space.com/21925-james-webb-space-telescope-jwst.html
- Really big infrared sensor
- Same questions apply.

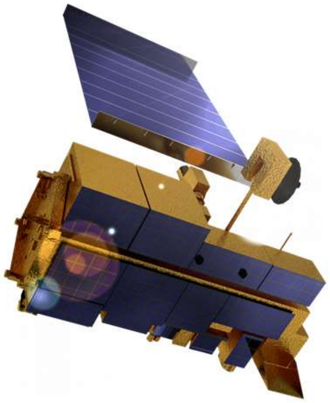


RoSat

- In 1998 a joint German / US X-ray sensor satellite called ROSAT was compromised.
- Allegedly involved a foreign actor gaining access to Goddard Space Flight Center via social engineering and poorly configured FTP services.
- Ultimately the actor was able to access a server that contained RoSat mission files. Algorithms were changed in those files that resulted in the satellite pointing towards the sun and overheating.
- The team was able to identify the issue and correct the satellites positioning but without knowing it was the result of cyber activity.
- Later it appears the actor came back, this time pointing the imager directly at the sun and permanently damaging it.

Landsat / Terra Sat

- October 2007 and July 2008, NASA-managed Landsat-7 satellite experienced 12 or more minutes of interference
- June and October 2008, Terra AM-1 satellite was disrupted for two minutes and nine minutes respectively
- The malicious activity was tied to a compromised ground station in Norway via local internet
- According to NASA the hackers had the full ability to send legitimate command and control tasking to the satellites from the compromised ground station



That disclosure problem…

- Skynet
  - Allegedly, a GROUP of computer hackers suspected of seizing control of a British military communications satellite using a home computer, triggering a "frenetic" security alert, has been traced to the south of England.
  - Allegedly, a security source said that, up to a month ago, the hackers found a "cute way" into the control system for one of the Ministry of Defence's Skynet satellites and "changed the characteristics of channels used to convey military communications, satellite television and telephone calls".
  - Allegedly, the facts as reported are as follows: Two weeks ago, British aerospace authorities noticed an irregularity in the position of one of their satellites, a military communications satellite belonging to a group of four known as Skynet satellites. Shortly thereafter, they received an anonymous message demanding money in exchange for control over the satellites guidance systems. "This is a nightmare scenario," an "intelligence source" told Reuters. "This is not just a case of computer nerds mucking about," said another. "This is very, very serious and the blackmail threat has made it even more serious.“
- NOAA
  - 2014 compromise of multiple aspects of their weather networks including space systems
  - Delayed reporting the breach and declined to comment on the extent of impacts of the compromise

But…….INSAT-4B Happened

- Credit to Jeffrey Carr and his Forbes article:
  - On July 7, 2010, a power glitch in the solar panels of India's INSAT-4B satellite resulted in 12 of its 24 transponders shutting down
  - India's Space Research Organization was a Siemens customer
  - According to the resumes of two former engineers who worked at the ISRO's Liquid Propulsion Systems Centre, the Siemens software in use is Siemens S7-400 PLC and SIMATIC WinCC, both of which will activate the Stuxnet worm.
  - https://www.forbes.com/sites/firewall/2010/09/29/did-the-stuxnet-worm-kill-indias-insat-4b-satellite/?sh=2618bb7a127d
- Regardless of conjecture and intended purpose, is proof that a state cyber campaign could effectively target space assets. Also, only example of true malicious code execution.

Constellations and Meshes: Mitigation or Risk?

- Pros
  - Additional satellites can improve resilience
  - Mesh network makes communications and tasking more r
  - Persistence more easily achieved
  - Less ground infrastructure
- Cons
  - Aggregation of risk
  - Enemy needs less infrastructure on the ground
  - Attacks can spread more quicky and have higher payoff

The Expectation of Protection

- Realistic:
  - Borders
  - Airspace
  - National Waters
- Unrealistic:
  - Cyber
  - Space

The Age of Space Conflict Asymmetry

WHAT WAS: Near peer adversaries capable of spaceflight contesting dominance of the space domain

WHAT IS: Anyone with a laptop and access to the internet has an ability to participate