FINAL FRONTIER SECURITY

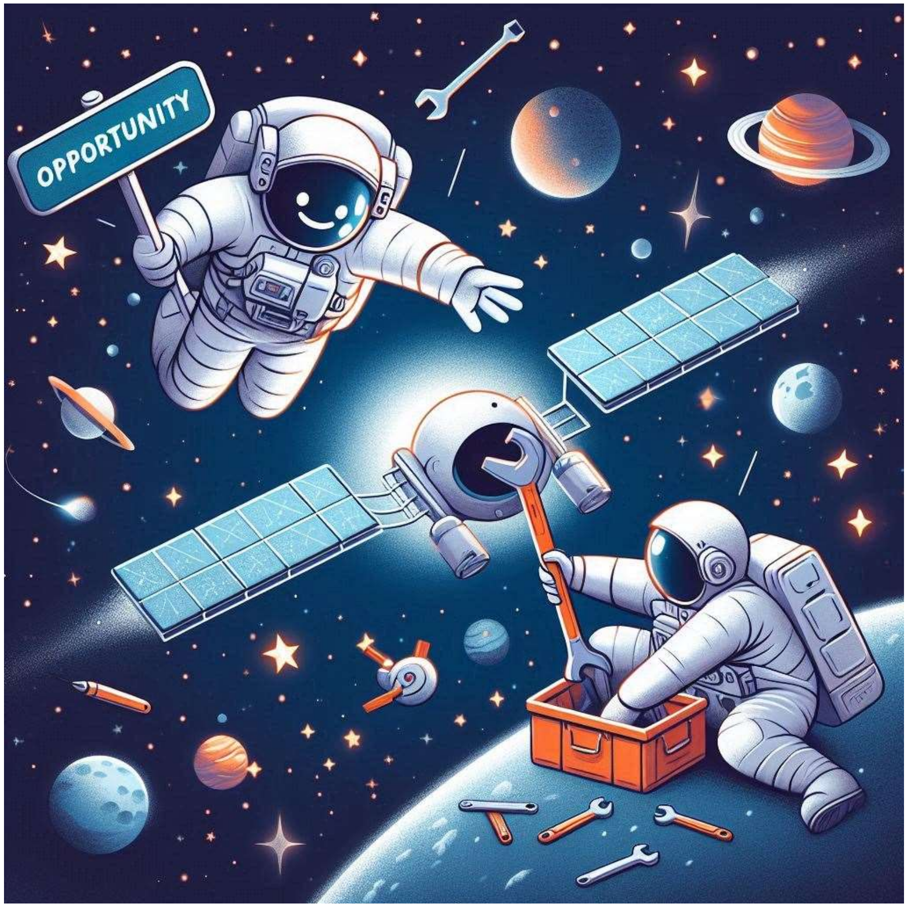
Lecture Four

The Future

Opportunity and Challenges

Opportunity and Difficulty

- Much of what constitutes the opportunity of cybersecurity for space systems is based round the aspects of the space domain that also make it difficult to provide solutions for.
- Will require not only an appreciation and understanding of the foundational issues but an ability to leverage them to inform cybersecurity R&D, implementations and operations.



Technical Difficulties

- Execution requires expertise in cybersecurity and aerospace
- Testing and evaluating solutions is extremely technical, expensive, and has limited capable institutions compared to traditional cybersecurity products
- Gaining experience in the field is rare and difficult, but becoming easier
- Managing resource utilization and risk mitigation has little precedent

Contrasting Space & SCADA / IoT

- We get to pace the space industry vs coming in decades later
- Many technologies resemble SCADA related tech, IoT, OT, but are more constrained
- Investing in SCADA/IoT talent has high ROI due to customer base
- Investing in aerospace expertise most be much more ROI conscious

Space Rated/Hardened/Resilient Parts

- That’s right, sometimes normal off the shelf stuff passes enough testing to get launched into space
- So, do I need to test my cybersecurity solution on expensive long lead space parts or no?
- The answer is maybe, it depends
- Radiation, latch ups & physical vs logical mitigations and impacts on cybersecurity implementation
  - Backups / Gold Images

Big (old) vs Small (new)

- Big:
  - Vertically integrated
  - Provide their own solutions
- Small
  - Outsourcing of test, evaluation, etc

Heritage is King, Heritage is Hard

- Space customers and the industry as a whole are obsessed with heritage
- It is expensive to put stuff into space
- It s hard to put stuff into space
- For SW there are more options for establishing heritage
  - ISS, rideshare, old / unused birds, colleges etc
- For HW, this is a much harder problem, but establishing heritage here could be golden

WHAT IS MY PURPOSE?
CYBERSECURITY...
OH MY GOD
imgflip.com

The Challenge of Space System Cybersecurity: Architecture

- Telemetry can be used for anomaly detection, just like on systems such as other critical infrastructure / SCADA
- Marrying telemetry to traditional threat hunting is a novel-ish way to approach cybersecurity for space
- Need to understand the potential folly in relying on standard data from the vehicle if it is compromised
- Using something like visual tracking etc. maybe only reliable method to pare the two

Space Rating Cybersecurity

- UAH SSD
- STARGATE
- IEEE Standard

The University of Alabama in Huntsville demonstrates cybersecurity software aboard a Lockheed Martin technology demonstrator CubeSat

The Small Satellite Defender

- OCT 05, 2023, The University of Alabama in Huntsville (UAH) today announced that it developed a cybersecurity software for the U.S. Army Space and Missile Defense Command (USASMDC). The software began performance testing on one of Lockheed Martin's (NYSE: LMT) In-space Upgrade Satellite System (LM LINUSS™) technology demonstrator CubeSats. The software, Small Satellite Defender, is an intrusion detection system designed for small satellites.
- The Small Satellite Defender – created by UAH students, UAH Center for Cybersecurity Research and Education (CCRE) staff and USASMDC cybersecurity engineers – will continue to run for multiple weeks collecting data and periodically transmitting data to the ground station. The students are members of the Space Testing and Resiliency Simulation team, or STARS, who perform small satellite research and development for USASMDC
- The Small Satellite Defender runs with relatively low power, monitors for satellite specific threats and requires very low bandwidth. The software is collecting data for multiple weeks and periodically transmitting the cyber status to the ground station. The initial test results indicate the Small Satellite Defender software performed as intended, and the application passed all in-flight tests.
- https://www.uah.edu/news/news/the-university-of-alabama-in-huntsville-demonstrates-cybersecurity-software-aboard-a-lockheed-martin-technology-demonstrator-cubesat

Space Rating The Small Satellite Defender

- Rating resource consumption
  - Aids in addressing system owner concerns
  - Command / configuration specific measurement
- If HW, Self-reliant housekeeping
  - Can’t rely on SV protections
- Data routing
  - Same as payload? As telemetry? As its own channel? Unique priority?

STARGATE

- Fictional but possible space craft cyber operations tool made from LANtenna and Etherify tools.
- Airgap jumping, segmentation defeating sniffer as well as potential bi-directional communications s
- https://www.bankinfosecurity.com/lantenna-attacks-exploit-air-gapped-networks-via-ethernet-cables-a-17688
- https://arxiv.org/pdf/2110.00104.pdf
- https://lipkowski.com/etherify/
- https://github.com/sq5bpf/etherify
- https://www.rtl-sdr.com/snooping-network-traffic-from-lan-cables-with-an-rtl-sdr-or-hackrf/
- https://www.rtl-sdr.com/etherify-transmitting-morse-code-via-raspberry-pi-ethernet-rf-leakage/

LANtenna

- "Ethernet cable emits electromagnetic waves in the frequency bands of 125 MHz. Changing the adapter speed or turning it on and off makes it possible to regulate the electromagnetic radiation and its amplitude," says Guri.
- In this case, data could be transmitted from an air-gapped computer through its Ethernet cable and received 200 cm apart, he says, adding that the signal was wrapped around 125.010 MHz.
- His research also showcases how a standard software-defined radio receiver in the area could decode the information and pass it to the attacker using internet.

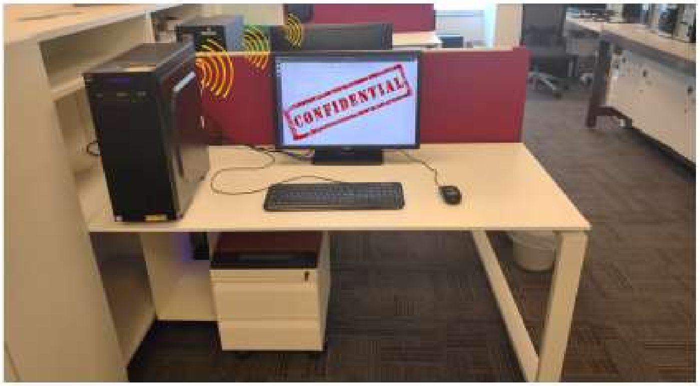


Fig. 1. Illustration of the LANTENNA attack. Malware in the air-gapped network exploits the Ethernet cable, using it as an antenna to transmit radio signals. Binary information is modulated on top of the signals and intercepted by a nearby radio receiver.

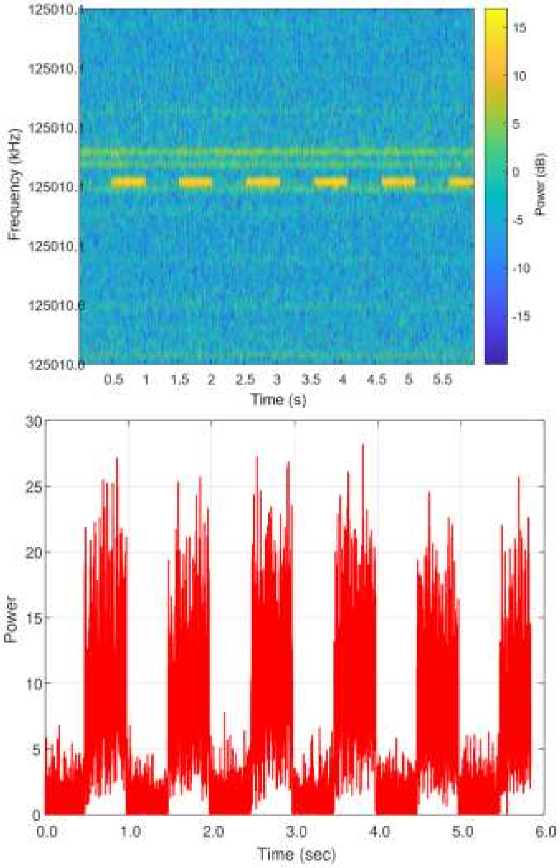
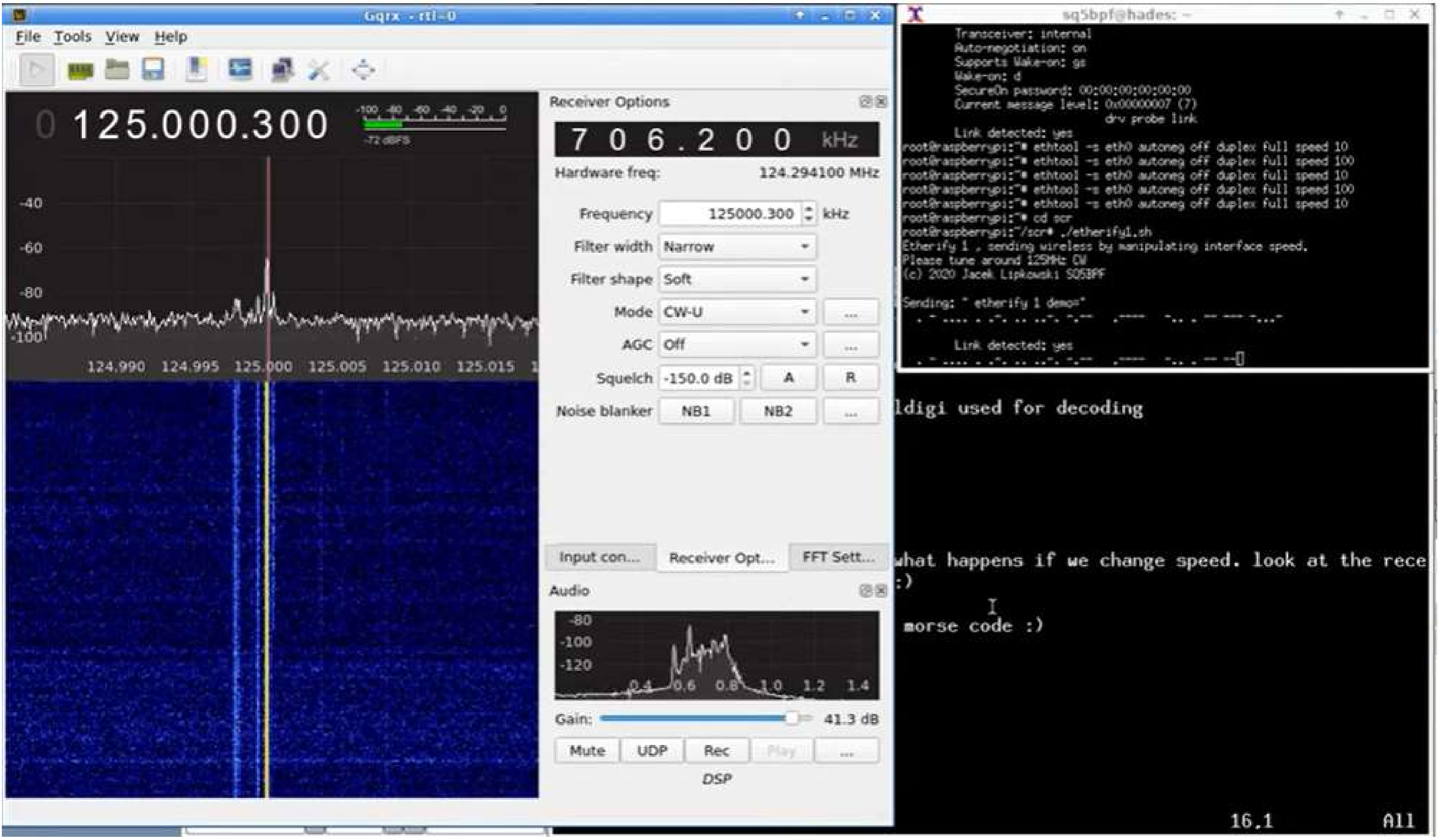


Fig. 2. The waveform and spectrogram generated by a transmission of the alternating sequence '0101010...' from the Ethernet cable, using the Ethernet speed toggling.

Etherify



Hardware freq: 124.294100 MHz

Frequency: 125000.300 kHz

Filter width: Narrow

Filter shape: Soft

Mode: CW-U

AGC: Off

Squelch: -150.0 dB

Noise blanker: NB1 NB2

Gain: 41.3 dB

```
        Transceiver: internal
        Auto-negotiation: on
        Supports Wake-on: gs
        Wake-on: d
        SecureOn password: 00:00:00:00:00:00
        Current message level: 0x00000007 (7)
                               drv probe link
        Link detected: yes
root@raspberrypi:~# ethtool -s eth0 autoneg off duplex full speed 10
root@raspberrypi:~# ethtool -s eth0 autoneg off duplex full speed 100
root@raspberrypi:~# ethtool -s eth0 autoneg off duplex full speed 10
root@raspberrypi:~# ethtool -s eth0 autoneg off duplex full speed 100
root@raspberrypi:~# ethtool -s eth0 autoneg off duplex full speed 10
root@raspberrypi:~# cd scr
root@raspberrypi:~/scr# ./etherify1.sh
Etherify 1 , sending wireless by manipulating interface speed.
Please tune around 125MHz CW
(c) 2020 Jacek Lipkowski SQ5BPF

Sending: " etherify 1 demo="
  . - .... . .-. .. ..-. -.--  .----  -.. . -- --- -...-

        Link detected: yes
  . - .... . .-. .. ..-. -.--  .----  -.. . -- --
```

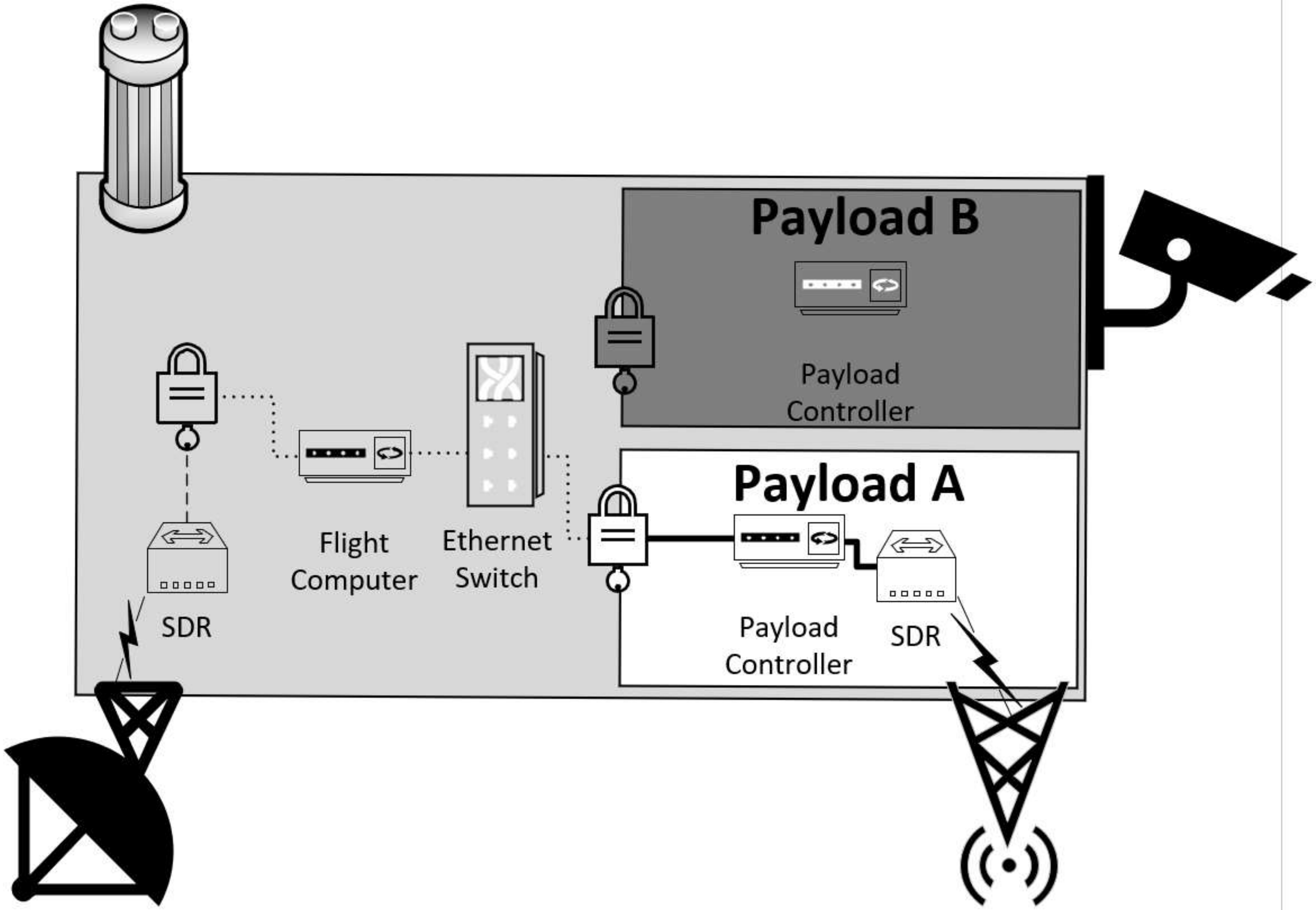
```
ldigi used for decoding



what happens if we change speed. look at the rece
:)

 morse code :)

                                          16,1          All
```


Payload B
Payload Controller
Flight Computer
Ethernet Switch
SDR
Payload A
Payload Controller
SDR

Space Rating STARGATE

- Rating resource consumption
  - Make sure can stay covert and avoid detection by operators monitoring resource utilization
  - Monitor and reattribute resource utilization reporting to the ground
  - Command specific risks or measurements
- Scheduling activity
  - Asynchronously
  - Around aerospace constraints
- Data routing
  - Same as payload? As telemetry? As its own channel? Via attacker ground stations?

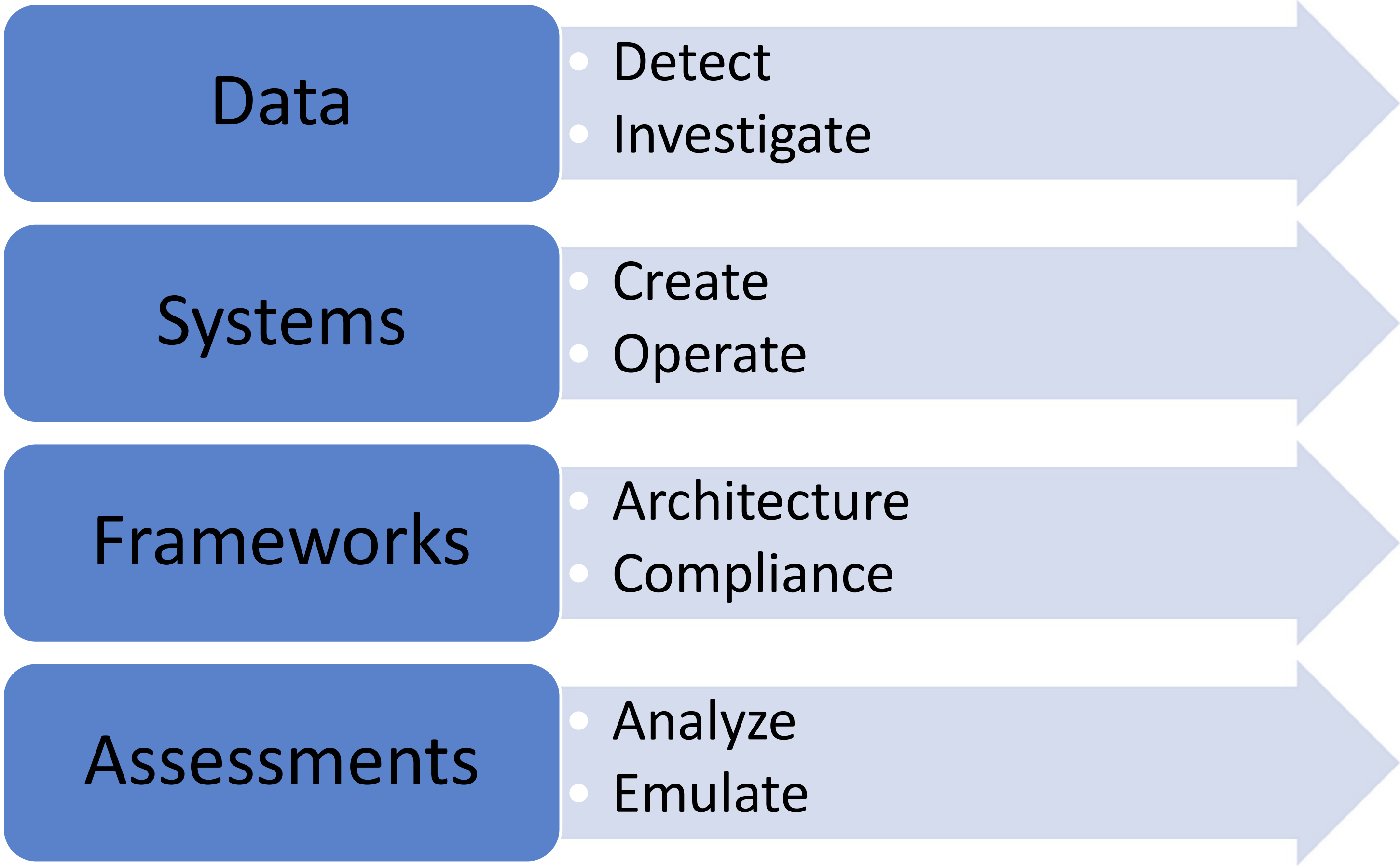
What should you test or assess?

- An actual satellite before launch
- All actual satellites before launch
- Flat sat
- Digital twin
- An orbiting satellite
- All orbiting satellites

Value proposition of Pen-Test / Red Team for space

- Those pesky problems
  - Modernization problem – dev's don't leverage security functions unless forced to
  - Disclosure problem – you cant rely on others to tip you to issues
  - Evaluation problem – case and point
  - Adaptation problem – exacerbating issue
  - Cyber warfare problem – adversarial mindset to protect adversaries
- Increased commercial entities that own operate and offer services increases potential for extortion, ransom etc
- Software supply chain will increasingly become a threat with COTS adaption
  - Solar Winds / Crowd Strike

Cybersecurity Roles



Data

- Detect
- Investigate

Systems

- Create
- Operate

Frameworks

- Architecture
- Compliance

Assessments

- Analyze
- Emulate

Data Roles & Space: Detect

- On the ground = traditional
- In space:
  - May have plenty of storage for extensive logging
  - Bandwidth competition with mission will prevent pulling down
  - CPU/ Memory may be capable of onboard analysis
    - Will likely compete with these as mission resources
    - Or; will compete with battery utilization
- Disclosure problem hurts effectiveness (lack of heuristics etc)

Data Roles & Space: Investigate

- On the ground = traditional + telemetry
- In space
  - To start, you don't get physical access
  - You may have to reverse engineer ways of doing system forensics as engineers will not think to need them as it relates to hacking activity
  - Your now competing with mission activity with each command or comms window you use to threat hunt or do forensics
- Most motivation & targeting by adversaries will likely be to disable or steal the asset so this will compound the disclosure issue as you don't get post mortem

System Roles & Space

- Create
  - Long system development lifecycles
  - Environmental constraints
    - Rad hardened (HW shielding / SW CONOPS)
    - ‘space rated’
    - Faults & avoidance
  - Operational constraints
    - Have to understand aerospace / system engineering and other industry specifics
- Operate
  - Competing with mission resources to conduct typical system operations
  - Have to understand aerospace / system engineering and other industry specifics

Frameworks Roles & Space

- Architecture

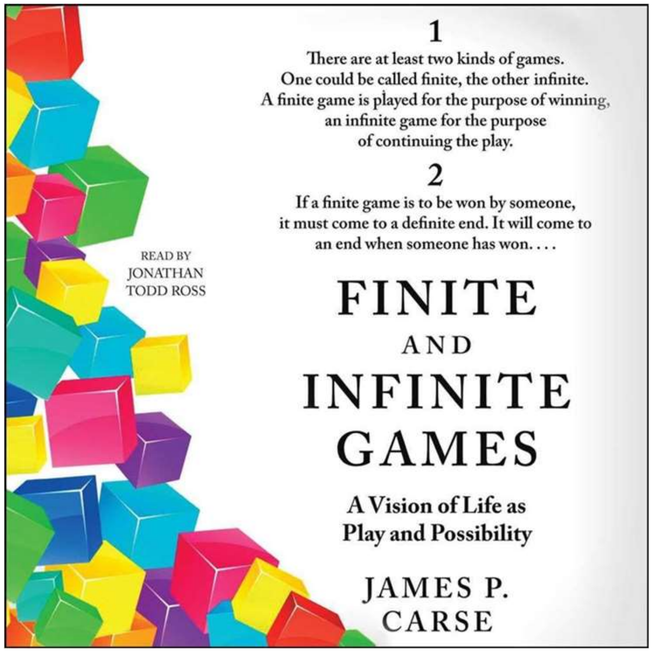
  Think back to the architecture discussion

- Compliance
  - RMF not good enough
  - Treating space systems as ‘appliance’
  - Good luck getting IVAV cycles / meeting windows for scans etc

Assessment Roles & Space

- Analyze
  - Requires space industry cultural understanding to convey analysis
  - Requires very unique niche system understanding
- Emulate
  - Despite our value proposition;
    - Where do you learn how to pentest these systems safely?
    - Where do you learn how to represent adversarial tradecraft adequately?
    - Where do you learn how to tell the right scary story

Infinite and Finite Games



1

There are at least two kinds of games.
One could be called finite, the other infinite.
A finite game is played for the purpose of winning,
an infinite game for the purpose
of continuing the play.

2

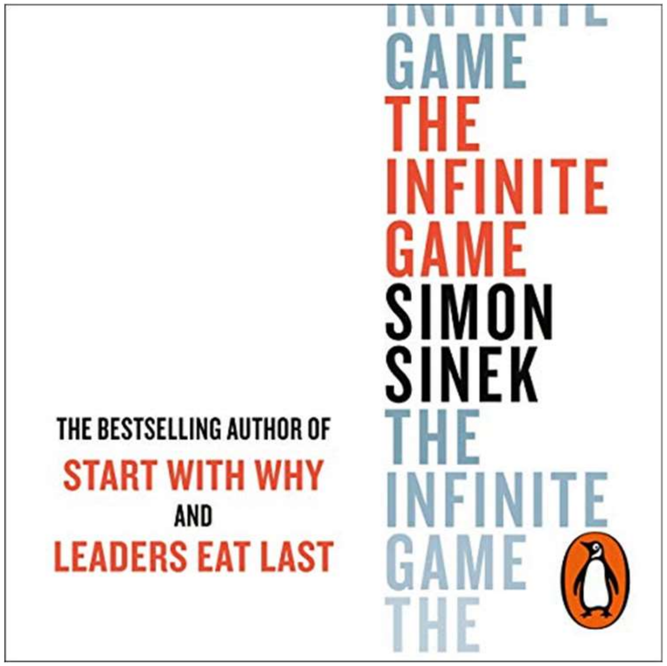
If a finite game is to be won by someone,
it must come to a definite end. It will come to
an end when someone has won. . . .

READ BY
JONATHAN
TODD ROSS

FINITE
AND
INFINITE
GAMES

A Vision of Life as
Play and Possibility

JAMES P.
CARSE



INFINITE
GAME
THE
INFINITE
GAME
SIMON
SINEK
THE
INFINITE
GAME
THE

THE BESTSELLING AUTHOR OF
START WITH WHY
AND
LEADERS EAT LAST

Cybersecurity is an Infinite Game

Cultural Shift

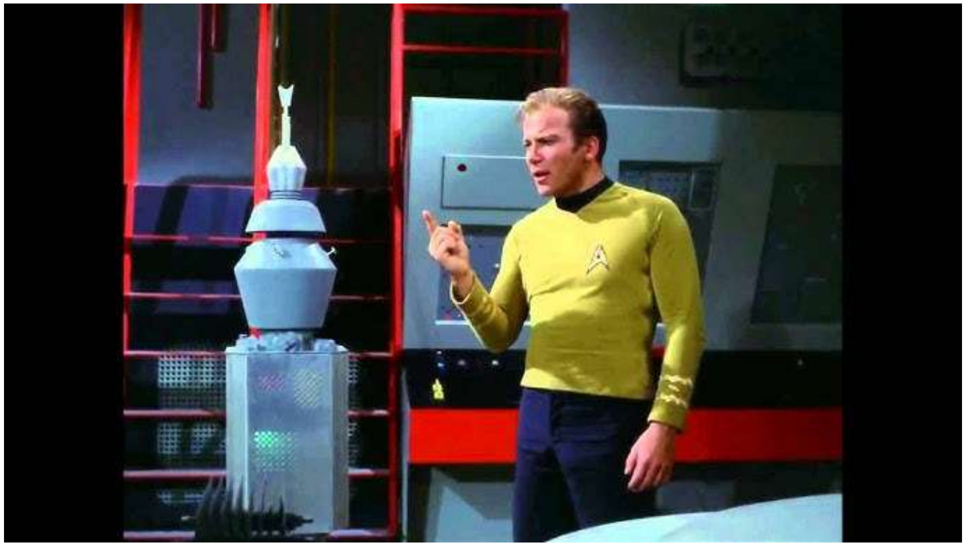
- The Cost benefit of Ransomware
  - Ransoming a big (MGM, Ceasers) is a bet
  - Ransoming many littles is more opportunistic
- Maersk & NotPetya; you don't even need to be the intended target
- A change in terminology
- A move towards resilience
- A challenge in IV&V

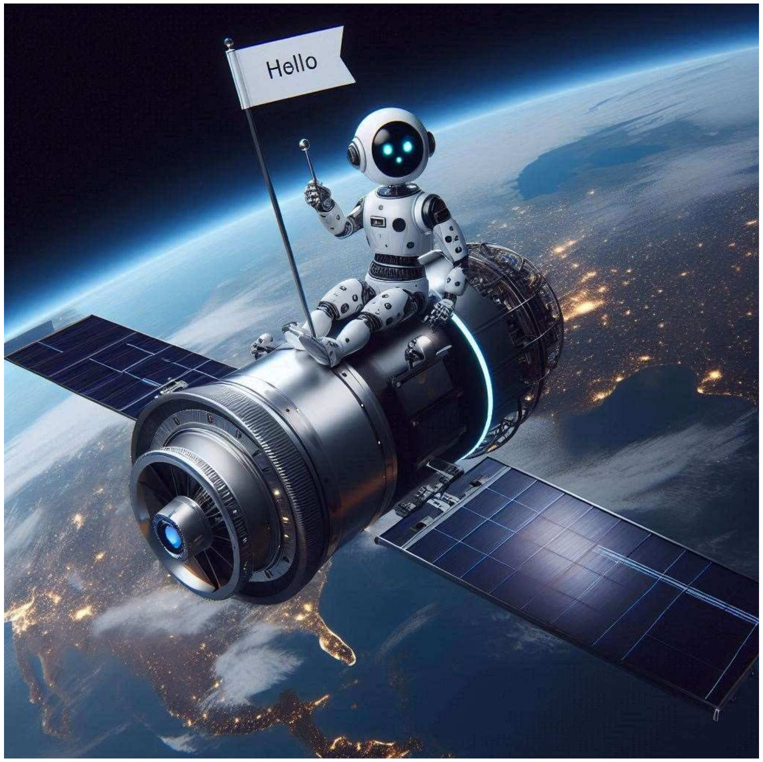
Infinite cyber and space systems

- Due to that theft potential, space may never be in a position of accepting and surviving compromise
- On the other hand, space engineering has a hyper focus on resilience and redundancy from a non cybersecurity perspective so it could also be considered suited to the infinite

Automation / AI / ML and SV's

- Execute missions with less need for commanding
- Problems can grow faster, go longer and be less correctable
- Introduces completely new attack surface
- Discussion





Maximizing Cost Benefit

- Fixing the warm squishy center

A path forward for cybersecurity in space

- Need to get past cybersecurity requirements and standards that can / are serviced by Engineers
- Cybersecurity as part of the engineering process
- The issue of demand signal may never be enough to service the niche
- Personal motivation, organizational culture that will drive excellence vs industry demand
- Cybersecurity for space will probably only be normalized once space is just like the internet, or cell phones, a taken for granted facet of everyday life