Introduction to Space System Vulnerabilities

Henry Reed

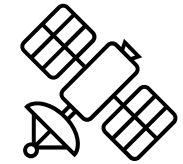
whoami

- Cybersecurity engineer with focus in the space industry
- SANS Technology Institute alumnus
- Certs:
  - OSCP
  - GPEN, GICSP, GCIH, GSEC
  - Others
- Previously spoke at CyberLEO, MTEM, BSides LV, ShellCon

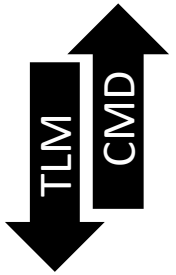
Outline

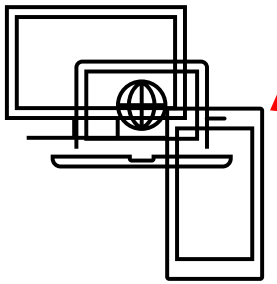
- Ground Station Network Architecture
- Ground Station Network Security
- Space Vehicle Architecture
- Space Vehicle Security
- Space Vehicle Exploitation
- Viasat: A Real-World Example
- How To Get Started

Ground Station Network Architecture



Space Vehicle

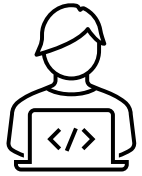




End User

- Commercial satellite imagery
- Weather news reports
- GPS receivers
- Satellite internet, phone, TV
- Governments (scientific, military)

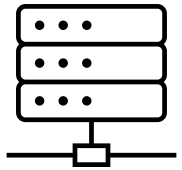
PAYLOAD DATA



MOC Operator

- MOC: Mission Operations Center
- Handles payload operations
- NASA sometimes calls this “Scientific Operations Center”, as their mission is scientific

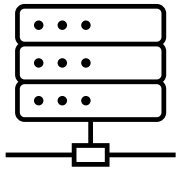
TLM
CMD



C2 Server

- AKA TT&C Server or Ground Station Software
- Receives CMD mnemonics from operators and sends it to the FEP
- Receives TLM from FEP, decodes it and forwards it to operators

TLM
CMD



Front End Processor

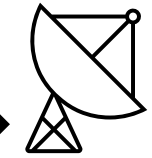
Digital signal processing, data recording, forward error correction

TLM
CMD

Crypto

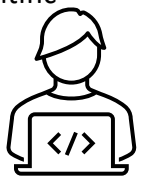
Caveat: Not everyone encrypts their CMD and/or TLM link ☹

TLM
CMD



Antenna

TLM
CMD

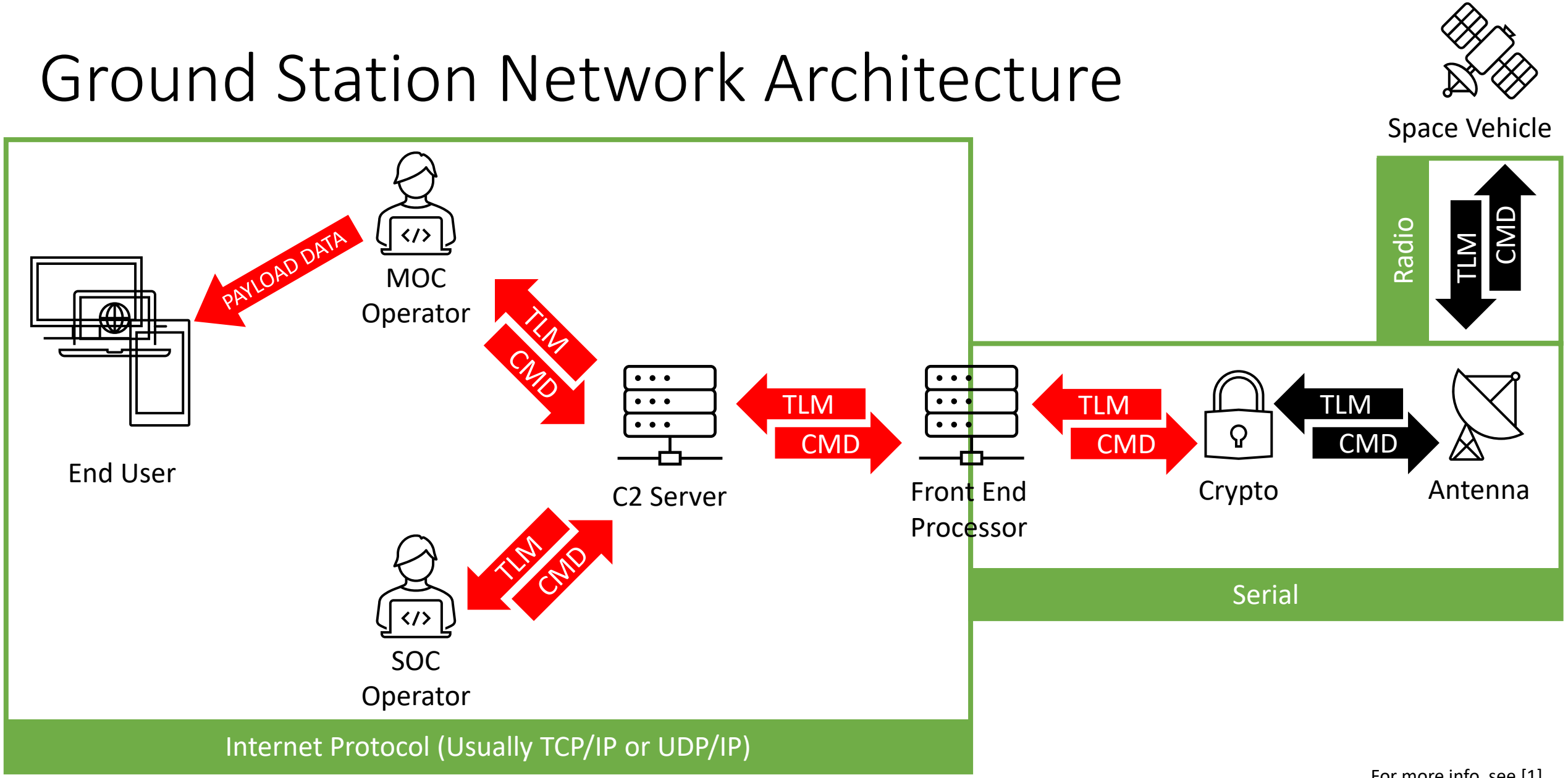


SOC Operator

- SOC: Space Operations Center
- Handles space vehicle operations
- Operator workstations run HMI software that connects to C2 server

For more info, see [1]

Ground Station Network Architecture



For more info, see [1]

Ground Station Network Security

- Very similar to securing an ICS Purdue Level 2 network, assuming 1 ground station
  - Arguably, Purdue Level 3 would be a plurality of ground stations; e.g., NASA's Deep Space Network
- Best case (not the current industry standard):
  - Host-based intrusion detection systems (AV, EDR) on workstations and servers
  - Network monitoring
  - Airgap with modern data diodes for user-segment-bound data
  - Two-factor authentication and authorization (e.g., smart cards)
  - Two-factor space vehicle telecommanding
  - Passive space vehicle telemetry and commanding cybersecurity monitoring
  - Industry-standard security hardening for each system configuration
    - E.g., hardening for Windows Active Directory Domain Controller if using one

Ground Station Network Security: C2 Server

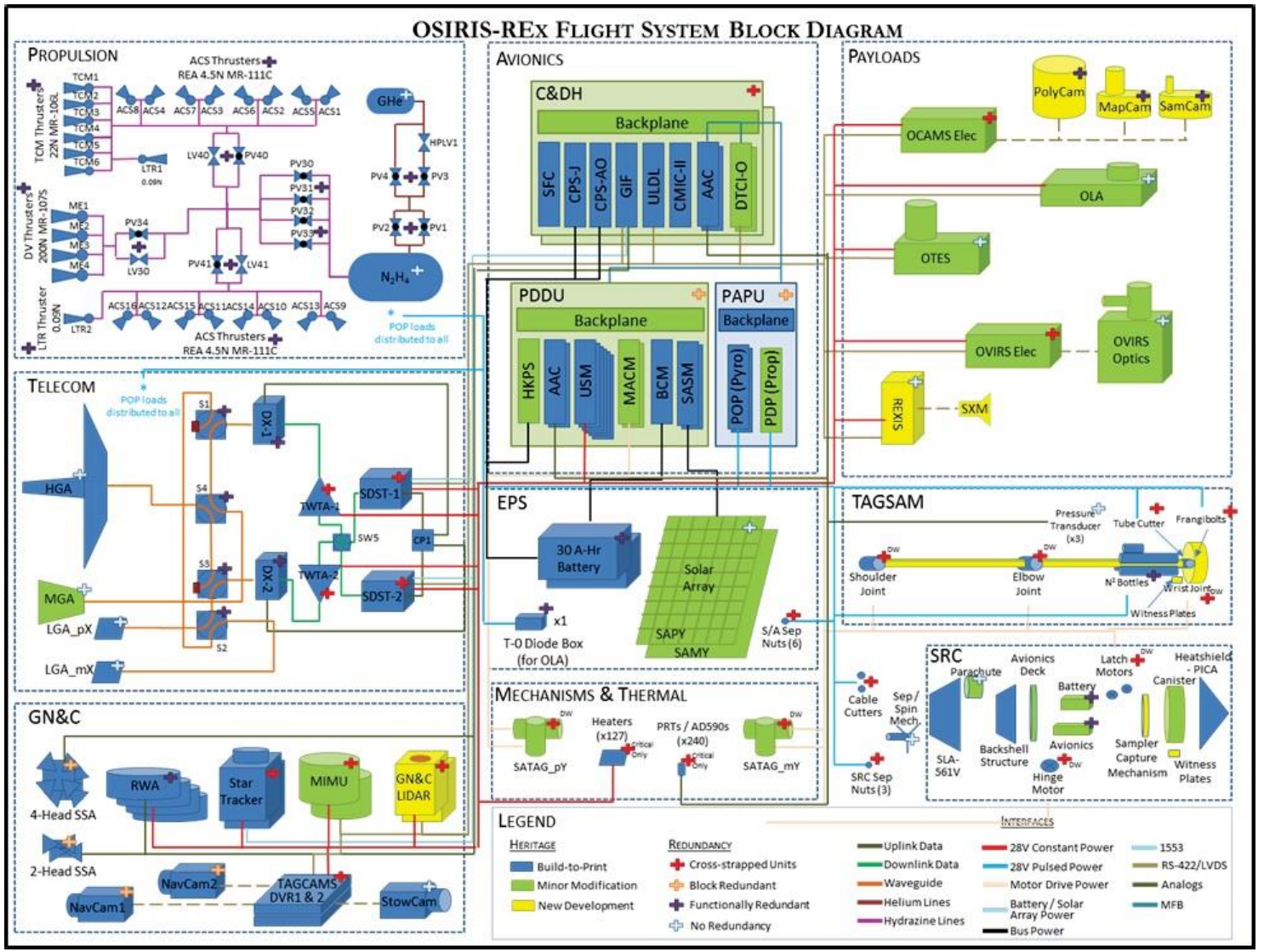
- Command and control servers may not have any user authentication built in
  - E.g., Ball Aerospace's COSMOS 4, which receives data over UDP/IP w/o authentication
  - Traditionally:
    - Operator workstation will require credentials; workstation comes with C2 client software (HMI) installed
    - C2 server assumes all data is trusted and comes from valid users
    - Network administrators assume no malicious operators are on the network
    - Very similar to other ICS environments
- If the adversary can get their hands on a copy of the C2 server, they can craft malicious packets to be sent directly to the space vehicle
  - Conversely: if an adversary can passively collect ground station network data, they can learn enough to send commands to the C2 server to attack the space vehicle w/o copy of C2 software
- Good C2 software will authenticate and authorize users at the network level

Ground Station Network Security: Others

- Lack of telemetry and command encryption, or insecure encryption
  - Allows for unauthorized command and control of a space vehicle
- Trusted relationship with compromised entity
  - Viasat KA-SAT network attack
- Supply-chain attacks
- Insider threats

Space Vehicle Architecture: OSIRIS-REx

- Uses MIL-STD-1553 serial bus
- Commons systems within a space vehicle:
  - G&NC or GNC: Guidance, Navigation and Control [2]; also known as:
    - ADCS or AD&C (Attitude Determination and Control System) [2]
    - AGS (Attitude Ground System) [2]
    - AOCS (Attitude and Orbit Control System) [2]
  - C&DH: Command and Data Handling
  - EPS: Electrical Power System
- Not uncommon to have monolithic flight software handle a majority of the above
- Various payloads



[3]

Space Vehicle Security

- Traditionally:
  - Only root user (let alone user authentication and authorization)
  - RTOS running very specialized, custom-built software
  - Payloads: separate hardware components for a single-purpose
    - E.g., NASA's Terra vehicle contains the ASTER payload, which conducts imagery collection via shortwave infrared (SWIR), thermal infrared (TIR) and visible and near infrared (VNIR)
    - E.g., SpaceX's Starlink vehicles contain RF payloads that only communicate with user-segment radio dishes to provide internet access
  - Payloads communicate with the command and data handling (C&DH) system; this is the main "flight computer"
  - Communication is done via a bus; e.g., MIL-STD-1553, SpaceWire, CAN, RS-422, and so on
    - Oftentimes there is no authentication or authorization within a spacecraft bus

Space Vehicle Security

- Flight software (FSW) options:
  - Custom built for the mission
  - Proprietary, but manufacturer-standard flight software
  - Free and open-source (FOSS) flight software (NASA cFS, ESA NMF, JPL F Prime, Stanford PyCubed) [4][5]
- Operating system:
  - GNU+Linux; Debian is officially in the list by NASA for Small Spacecraft State-of-the-Art [4]
  - FreeRTOS [4]
  - VXWorks [4]
  - RTEMS [4]
  - YoctoLinux [4]

Space Vehicle Exploitation via Valid CMDing

- Traditionally, flight software can be commanded to do just about anything:
- Overwrite the filesystem
  - Permanent denial of service (DoS) by overwriting boot partition, kernel, or other critical files
  - If software crypto is used, overwrite crypto keys
    - Space ransomware, anyone?
    - May also cause permanent DoS
- Overwrite memory
  - No point in finding a buffer overflow vulnerability if you can command the vehicle to overwrite any portion of memory as the root user
- Command the vehicle's GNC
  - Bad pointing or navigation can harm the mission; e.g., preventing a satellite internet vehicle from pointing towards the Earth will disrupt that internet connection for its users
- Command the vehicle's payloads
- Overwrite the filesystem of a vehicle's payload

Foreign ASAT Threats

- People's Republic of China
  - "[I]mplanting computer virus and logic bombs into the enemy's space information network so as to paralyze the enemy's space information system" is a valid strategy for China, according to Chinese military literature [6]
  - "[M]aintains a substantial kinetic ASAT [anti-satellite] capability" [7]
  - "Co-orbital technology demonstration's prove China's ability to rendezvous with other satellites in GEO [Geospatial Orbit] […] that demonstrate capability that is necessary for a co-orbital counterspace attack" [7]
  - "Solid foundation for potential cyber counterspace capabilities […] maintains significant space surveillance capabilities […] required to effectively target and employ their counterspace weapons" [7]
- Russian Federation
  - Nov. 2021, Russia tested DA-ASAT (direct-ascent anti-satellite) weapon system in low-Earth orbit [7]
  - Sept. 2018, "modified Russian MiG31 fighter jet was photographed carrying an unidentified missile that was reportedly a 'mock-up' of an air-launched ASAT weapon. Reports now suggest that this missile system is Burevestnik." [7]
  - Significant experience within the space industry [7]
  - Significant computer network exploitation and attack capability [7]; the Viasat KA-SAT attack was carried out by Russia [8][9]

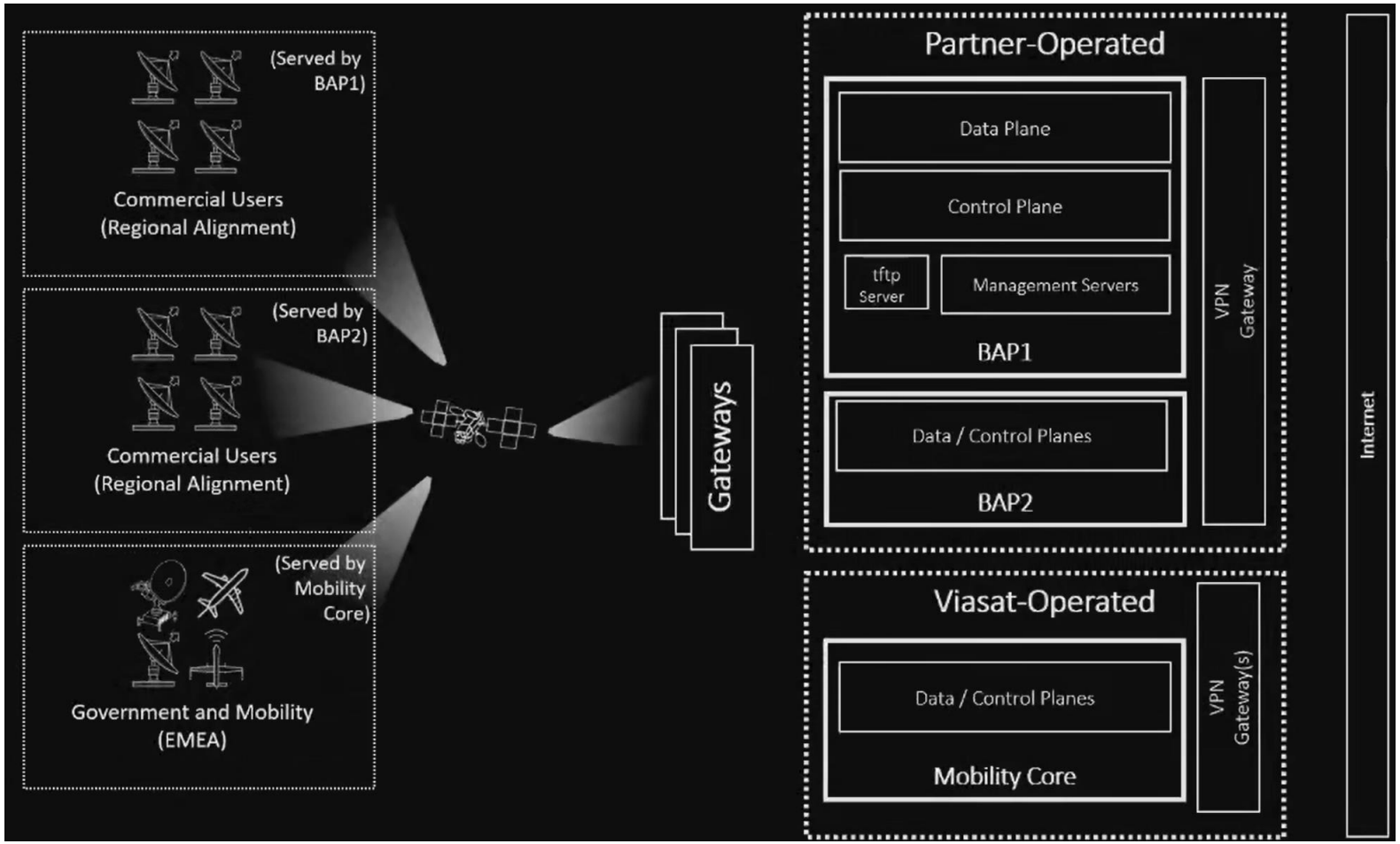
Case Study: Viasat KA-SAT Network Attack

- 24FEB22: Russian Federation invades Ukraine for the second time; RF/GRU attacks Viasat KA-SAT network
  - CNA attributed to Russia by European Union and its members, Australia, Canada, New Zealand, United Kingdom, United States [8][9]
  - CNA attributed to Russian GRU by Australia, Canada, New Zealand, United Kingdom, United States [9]
  - “Further specific national statements aligning with this attribution were made by the ministries of foreign affairs of Estonia, Denmark, Ireland, the Netherlands, Norway, Austria, Germany, Czechia, Italy, Finland, Romania, Poland, and France.” [9]
  - Day of the second invasion of Ukraine by Russia, part of the 2014 Russo-Ukrainian war [9]
- Impact: Civilian targets only [9]
  - Consistent with Russia’s kinetic warfare tactics, the attack against Ukraine primarily impacted non-military targets, knocking down communication for civilians in the beginning of the second invasion [9] [11] [12] [13]
  - Impacted energy systems across Ukraine and Europe [9]
  - Risk to human life

Image Credit: Apartment block in Kyiv (Oleksandr Koshyts Street, 7-A) after hitting by remains of a downed Russian missile during Russian invasion of © 2022 Ukraine Kyiv City Council, licensed CC BY 4.0

Case Study: Viasat KA-SAT Network Attack

- GRU conducted CNA against Viasat's partner-operated network, gaining access to the TFTP server that managed software updates for KA-SAT modems [9][10]
  - Space vehicles were NOT targeted in this attack; the attack was against the ground station and impacted satellite internet modems [10]
- GRU also conducted attack from compromised terminals; i.e., the user segment [9][10]
  - Space vehicles, again, were NOT targeted in this attack [10]



Resources to Get Started

- NASA's Core Flight System (cFS): https://github.com/nasa/cFS
- ESA's Nanosat MO Framework: https://github.com/esa/nanosat-mo-framework
- Stanford University's PyCubed: https://github.com/pycubed/software
- OpenSatKit: https://github.com/OpenSatKit/OpenSatKit
  - cFS bundled with a physics simulator and COSMOS 4 C2 software
- OpenC3: https://github.com/OpenC3/cosmos
  - Open-source alternative to Ball Aerospace's COSMOS 5
- COSMOS 4: https://github.com/BallAerospace/COSMOS/tree/v4.5.2
  - Open-source C2 software
- The Aerospace Corporation's SPARTA framework: https://sparta.aerospace.org

Citations

[1] OTR 2020-00393, **The Aerospace Corporation**, “Re-defining Success of Ground Cyber Assessments”, https://gsaw.org/wp-content/uploads/2020/03/2020s11g_bailey.pdf
[2] 20110007876, **NASA**, “Attitude Determination and Control Systems”, https://ntrs.nasa.gov/api/citations/20110007876/downloads/20110007876.pdf
[3] NO SERIAL, **NASA and Lockheed Martin Co.**, “OSIRIS-REx Spacecraft Functional Block Diagram”, https://spaceflight101.com/osiris-rex/osiris-rex-spacecraft-overview/
[4] NASA/TP—2022–0018058, **NASA**, “State-of-the-Art Small Spacecraft Technology”, https://www.nasa.gov/wp-content/uploads/2023/05/2022-soa-full.pdf
[5] SSC19-WKIII-04, **Stanford University**, “PyCubed: An Open-Source, Radiation-Tested CubeSat Platform Programmable Entirely in Python”, https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=4364&context=smallsat
[6] NO SERIAL, **U.S.-China Economic And Security Review Commission**, “2011 REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION”, https://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf
[7] NO SERIAL, **Center for Strategic and International Studies**, “Space Threat Assessment 2023”, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-04/230414_Bingen_Space_Assessment.pdf
[8] NO SERIAL, **DoS**, “Attribution of Russia’s Malicious Cyber Activity Against Ukraine”, https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/
[9] NO SERIAL, **Cyber Peace Institute**, “Case Study: Viasat”, https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat
[10] NO SERIAL, **Viasat**, “Defending KA-SAT”, https://youtu.be/qI_ICtX3Gm8
[11] NO SERIAL, **The New York Times**, “Calculating the Toll of Russia’s War on Ukrainian Culture”, https://www.nytimes.com/interactive/2022/12/19/arts/design/ukraine-cultural-heritage-war-impacts.html
[12] NO SERIAL, **The New York Times**, “When Cultural Heritage Becomes a Battlefront”, https://www.nytimes.com/2022/12/27/arts/design/cultural-heritage-ukraine-russia-war.html
[13] NO SERIAL, **The New York Times**, “Russia Repeatedly Strikes Ukrainian Civilians. There’s Always an Excuse.”, https://www.nytimes.com/article/russian-civilian-attacks-ukraine.html