Protecting Space Capabilities: Securing Our Advantage in the Tactical Battlespace

COL BE Rhodes

Roles: Industry/Military/Academia

November 2021

Outline

- WHOIS
- Where to begin?
- Foundations
- Tactical Space Capabilities
- Space-Cyber Intersections
- Threats & Impacts
- Where do we go from here?

WHOIS: Brad Rhodes

- WHOIS: Brad Rhodes
- TLDR:
  - ✓ Head of Cybersecurity at zvelo
  - ✓ COL, Cyber (17A), 76th Operational Response Command G6/CIO
  - ✓ Military Cyber Professionals Association, HammerCon Co-Lead
  - ✓ Speaker, Author, Professor, Coach
  - ✓ #toomany Pro-Certs, highlights: CISSP-ISSEP, CISM, CDPSE, PMP, CEH, GMON, GCIH, Cloud+, CySA+

Feel to view/listen/grab my previous presentation/articles here:
https://github.com/cyberguy514

Where to begin?

- The last 18+ months have been nuts!
  - A global pandemic
  - Lockdowns & restrictions
  - Massive shift to work from home / remote work
  - Emboldened malicious cyber actors (MCA)
  - Medicine and vaccine scams
  - Misinformation on just about everything
  - US Presidential election
  - US Capitol attack
  - Afghanistan withdrawal
  - Growth in commercial space launch
  - More and more small sats

Captain Kirk went to space!!

Foundations: Joint Pub 3-14 (Space Operations)

- The relationship between space and cyberspace is unique in that many **space operations depend on cyberspace**, and a critical portion of cyberspace can only be provided via space operations.
- Similar to air, land, and maritime operations and forces, space operations and forces are **interconnected with cyberspace** through the Electro-magnetic Spectrum (EMS).
- Cyberspace provides a means for satellite control and spacecraft **data transport**. The transport layer is critical, and the linkages must be addressed during planning and operations to ensure cyberspace concerns are met.
- Satellites and **ground systems are vulnerable to cyberspace threats** (i.e., code modification, encryption defeat, and other intrusion methods).
- Indications and warning of a cyberspace attack against space systems requires special attention, as the **overlap of space and cyberspace** provides an effective avenue to attack space systems.

Cyber is mentioned 44 times!

Foundations: Field Manual 3-14 (Army Space Operations)

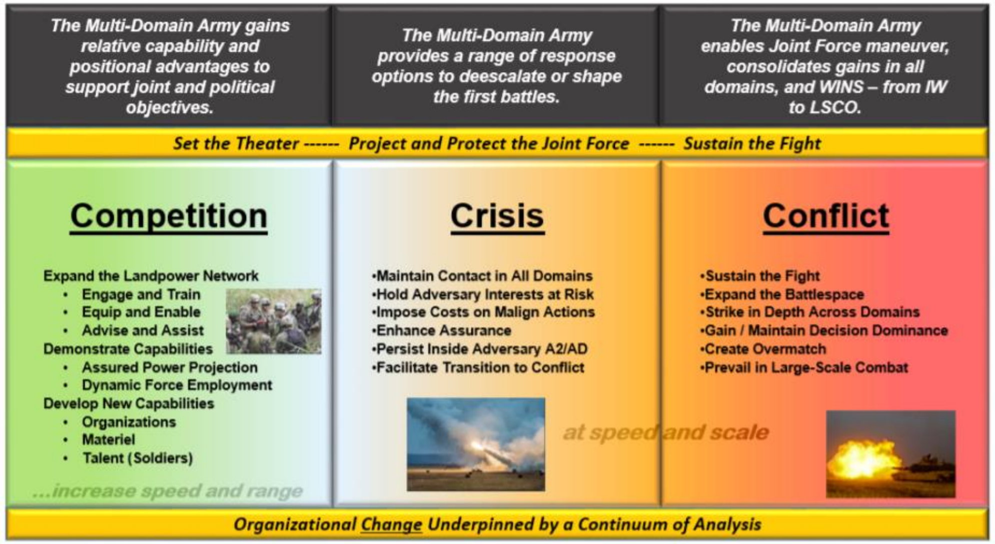
- Space capabilities permit enhanced situational understanding; provides global communications; enables precise and accurate fires; supports the conduct of joint expeditionary entry, movement, and maneuver operations; and **provides a conduit for cyber electromagnetic operations** supporting Unified Land Operations
- **Cyberspace operations protect friendly networks** that leverage GNSS, while targeting similar adversary capabilities.
- The space domain supports and enables all other domains—it is interdependent with the air, land, and maritime domains, and **interconnected with the cyberspace domain**.
- The **EMS crosses all domains**, and it provides a vital link between the cyberspace and space domains.
- Cyberspace attack targets the data and the systems dependent upon the data rather than the radio frequency band in which the information is transmitted. **Cyberattacks may target the ground stations, end-user equipment, or the satellites**.

Cyber is mentioned 73 times!

Tactical Space Capabilities

Army Space Capabilities

- SSA
- PNT
- Space control (DSC, OSC, NAVWAR)
- SATCOM
- Satellite operations
- Missile warning
- Environmental monitoring
- Space-based surveillance and reconnaissance



The Multi-Domain Army gains relative capability and positional advantages to support joint and political objectives.

The Multi-Domain Army provides a range of response options to deescalate or shape the first battles.

The Multi-Domain Army enables Joint Force maneuver, consolidates gains in all domains, and WINS – from IW to LSCO.

Set the Theater ------ Project and Protect the Joint Force ------ Sustain the Fight

Competition

Expand the Landpower Network
- Engage and Train
- Equip and Enable
- Advise and Assist

Demonstrate Capabilities
- Assured Power Projection
- Dynamic Force Employment

Develop New Capabilities
- Organizations
- Materiel
- Talent (Soldiers)

...increase speed and range

Crisis

- Maintain Contact in All Domains
- Hold Adversary Interests at Risk
- Impose Costs on Malign Actions
- Enhance Assurance
- Persist Inside Adversary A2/AD
- Facilitate Transition to Conflict

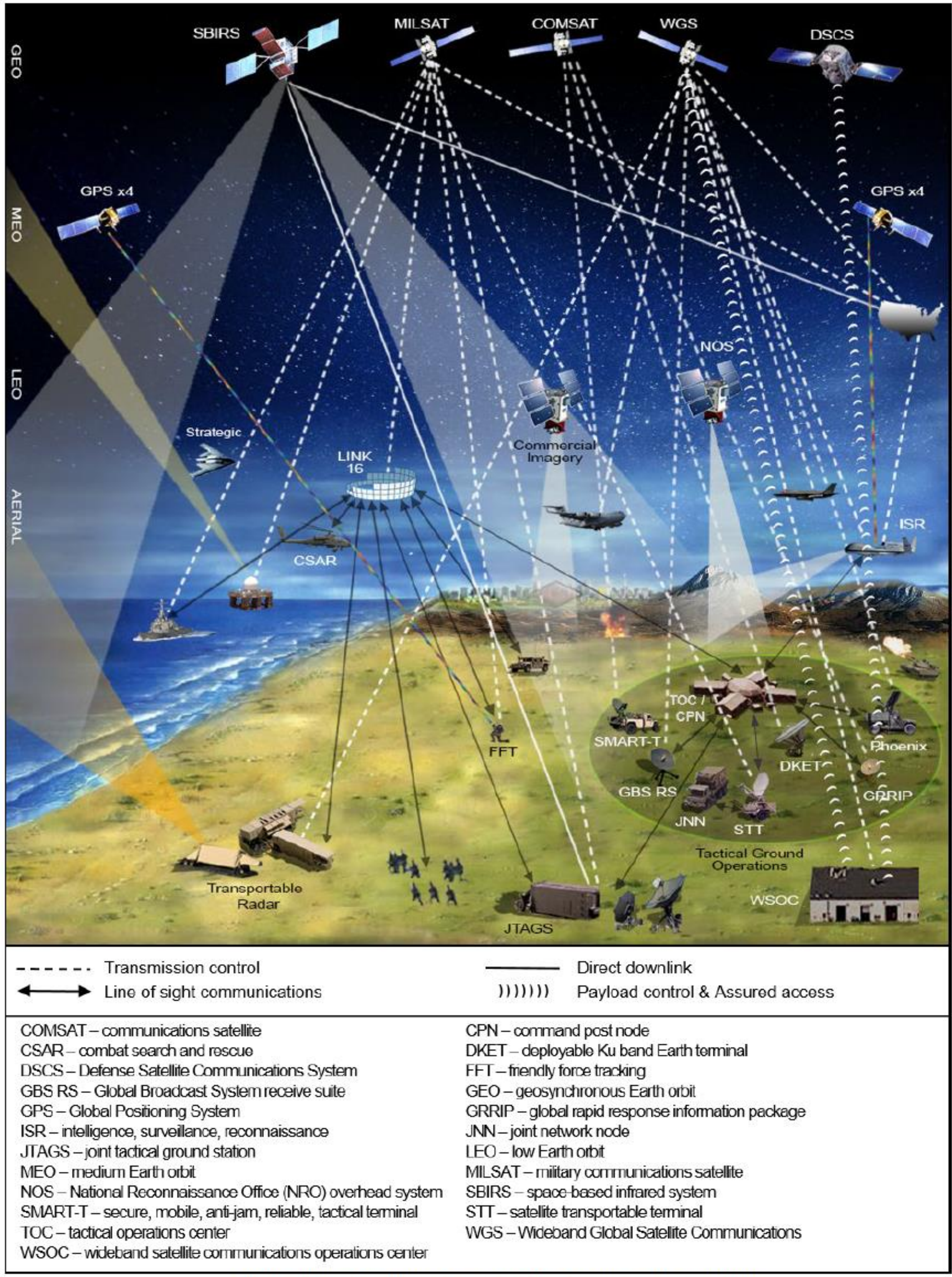
at speed and scale

Conflict

- Sustain the Fight
- Expand the Battlespace
- Strike in Depth Across Domains
- Gain / Maintain Decision Dominance
- Create Overmatch
- Prevail in Large-Scale Combat

Organizational Change Underpinned by a Continuum of Analysis

Ref: https://api.army.mil/e2/c/downloads/2021/03/23/eeac3d01/20210319-csa-paper-1-signed-print-version.pdf

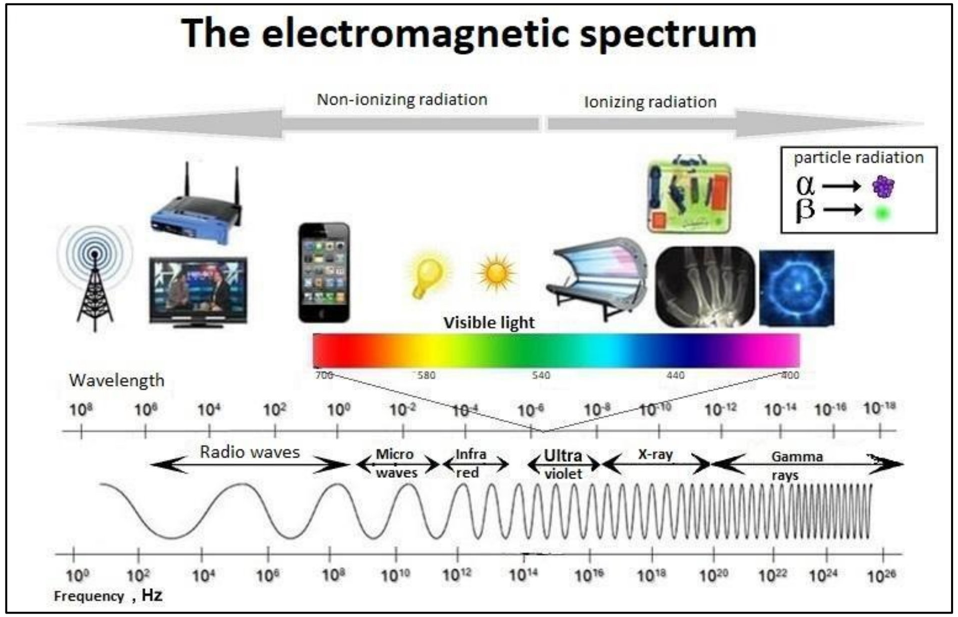


- - - - - -	Transmission control	———	Direct downlink
⟷	Line of sight communications	)))))))	Payload control & Assured access

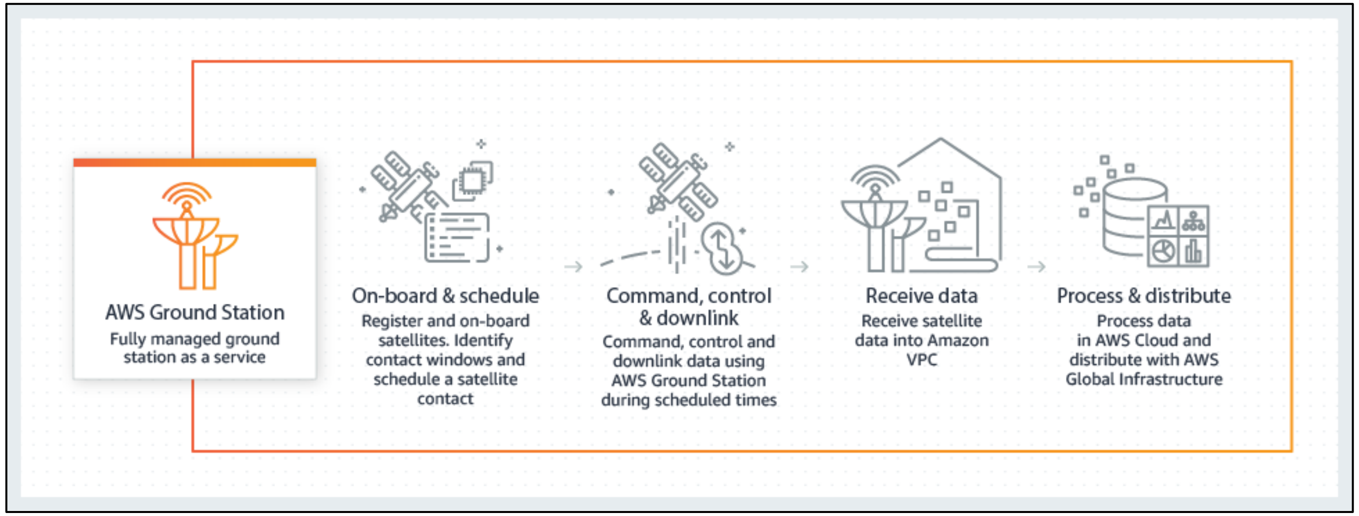
COMSAT – communications satellite
CSAR – combat search and rescue
DSCS – Defense Satellite Communications System
GBS RS – Global Broadcast System receive suite
GPS – Global Positioning System
ISR – intelligence, surveillance, reconnaissance
JTAGS – joint tactical ground station
MEO – medium Earth orbit
NOS – National Reconnaissance Office (NRO) overhead system
SMART-T – secure, mobile, anti-jam, reliable, tactical terminal
TOC – tactical operations center
WSOC – wideband satellite communications operations center
CPN – command post node
DKET – deployable Ku band Earth terminal
FFT – friendly force tracking
GEO – geosynchronous Earth orbit
GRRIP – global rapid response information package
JNN – joint network node
LEO – low Earth orbit
MILSAT – military communications satellite
SBIRS – space-based infrared system
STT – satellite transportable terminal
WGS – Wideband Global Satellite Communications

Figure 1-1. Army space operations concept overview

Space-Cyber Intersections



Ref: https://www.uib.no/en/hms-portalen/75292/electromagnetic-spectrum



AWS Ground Station
Fully managed ground station as a service

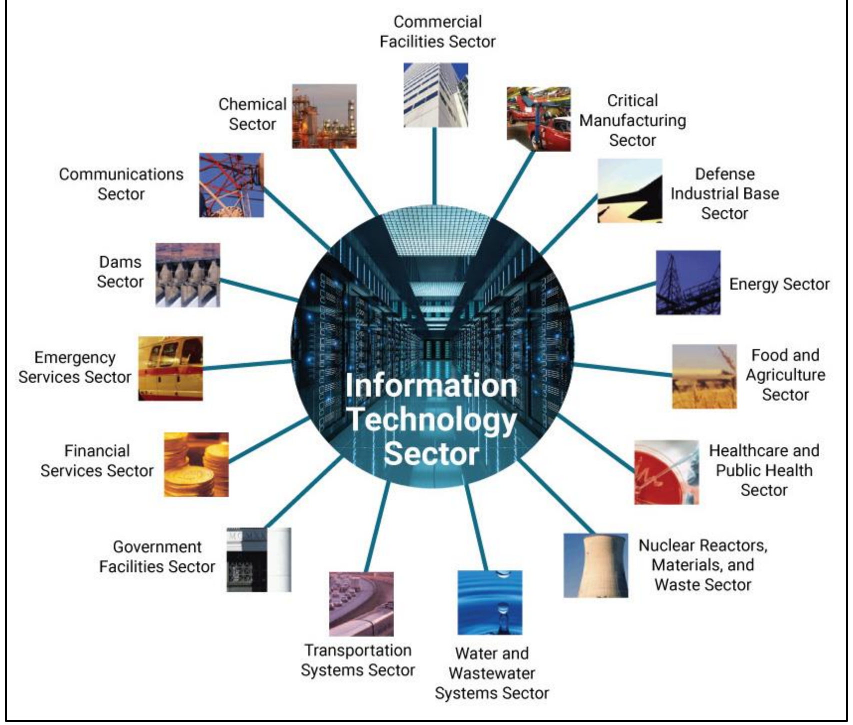
On-board & schedule
Register and on-board satellites. Identify contact windows and schedule a satellite contact

Command, control & downlink
Command, control and downlink data using AWS Ground Station during scheduled times

Receive data
Receive satellite data into Amazon VPC

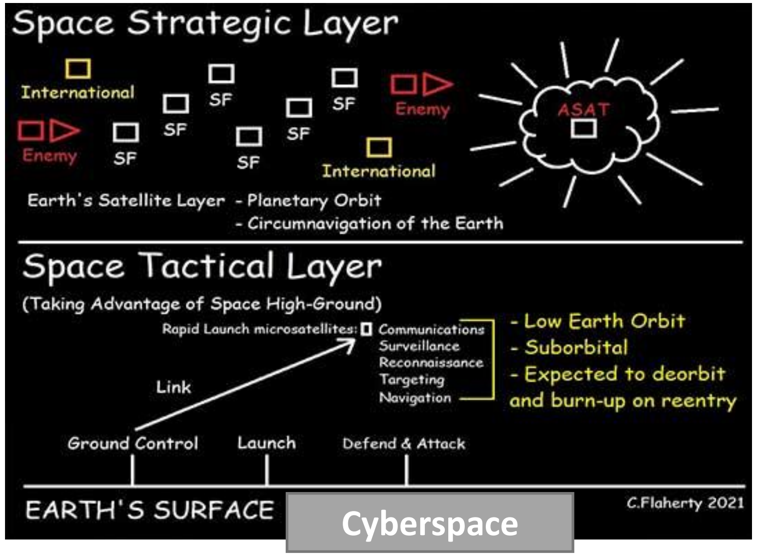
Process & distribute
Process data in AWS Cloud and distribute with AWS Global Infrastructure

Ref: https://aws.amazon.com/ground-station/



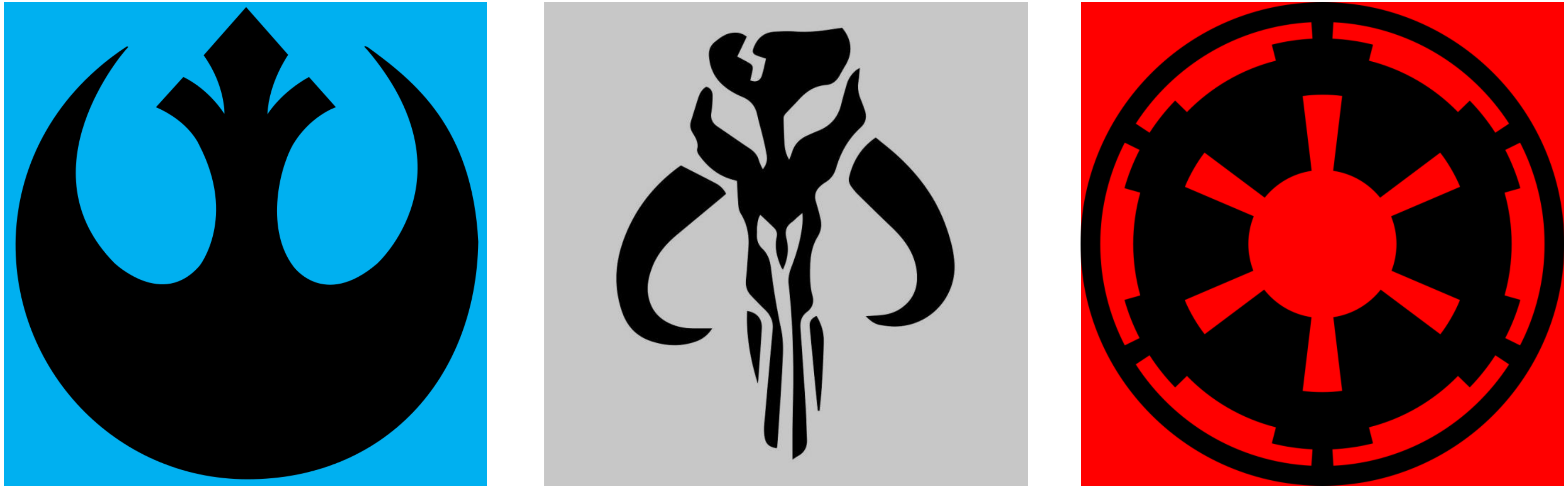
Information Technology Sector
Commercial Facilities Sector
Critical Manufacturing Sector
Defense Industrial Base Sector
Energy Sector
Food and Agriculture Sector
Healthcare and Public Health Sector
Nuclear Reactors, Materials, and Waste Sector
Water and Wastewater Systems Sector
Transportation Systems Sector
Government Facilities Sector
Financial Services Sector
Emergency Services Sector
Dams Sector
Communications Sector
Chemical Sector

Ref: https://securityboulevard.com/2019/12/how-to-cyber-security-software-is-critical-infrastructure/



Ref: https://spaceanddefense.io/the-space-tactical-layer/

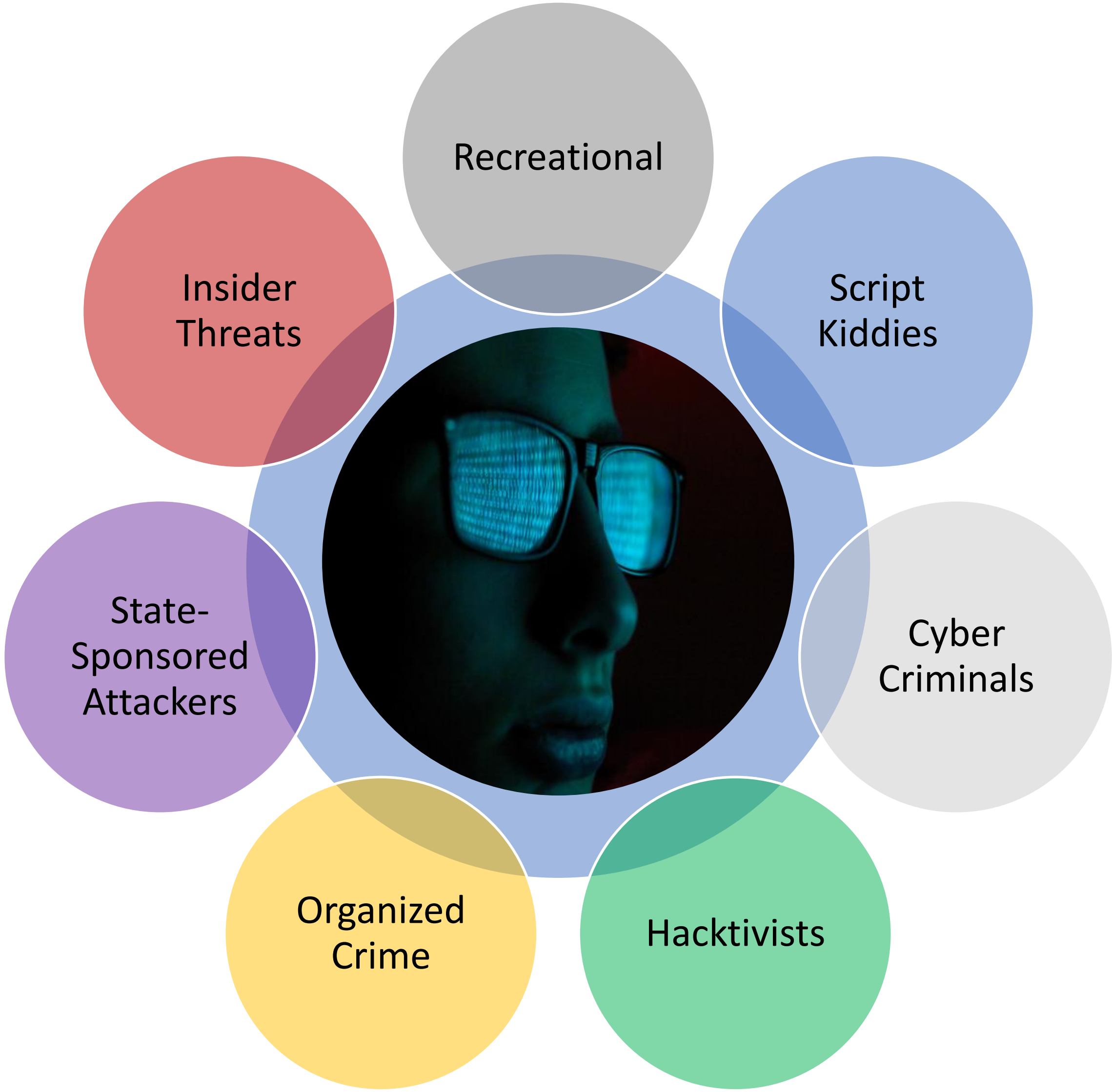
We pause for this public service announcement…



STANDARDS & TOOLS – SAME ONES USED BY BLUE, GRAY, & RED

Images: Copyright Disney/Lucasfilm

Threats & Impacts: Attacker “Families”

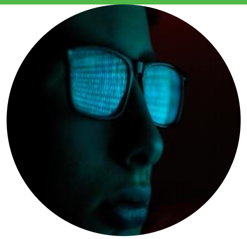


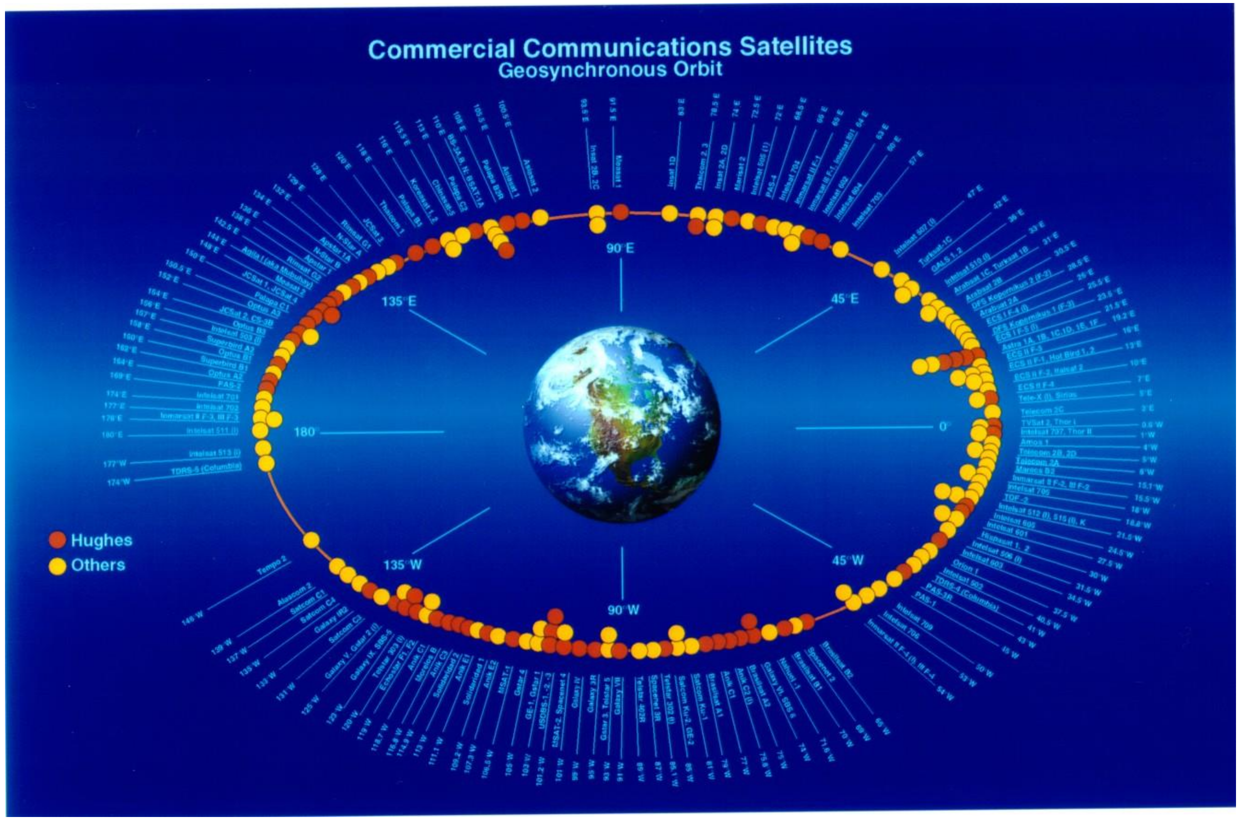
Raphael Mudge's
COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS
SC COMICS
Issue #1
I THOUGHT REAL HACKERS USED VULNERABILITY SCANNERS?
http://www.advancedpentest.com

Ref: https://www.cobaltstrike.com/

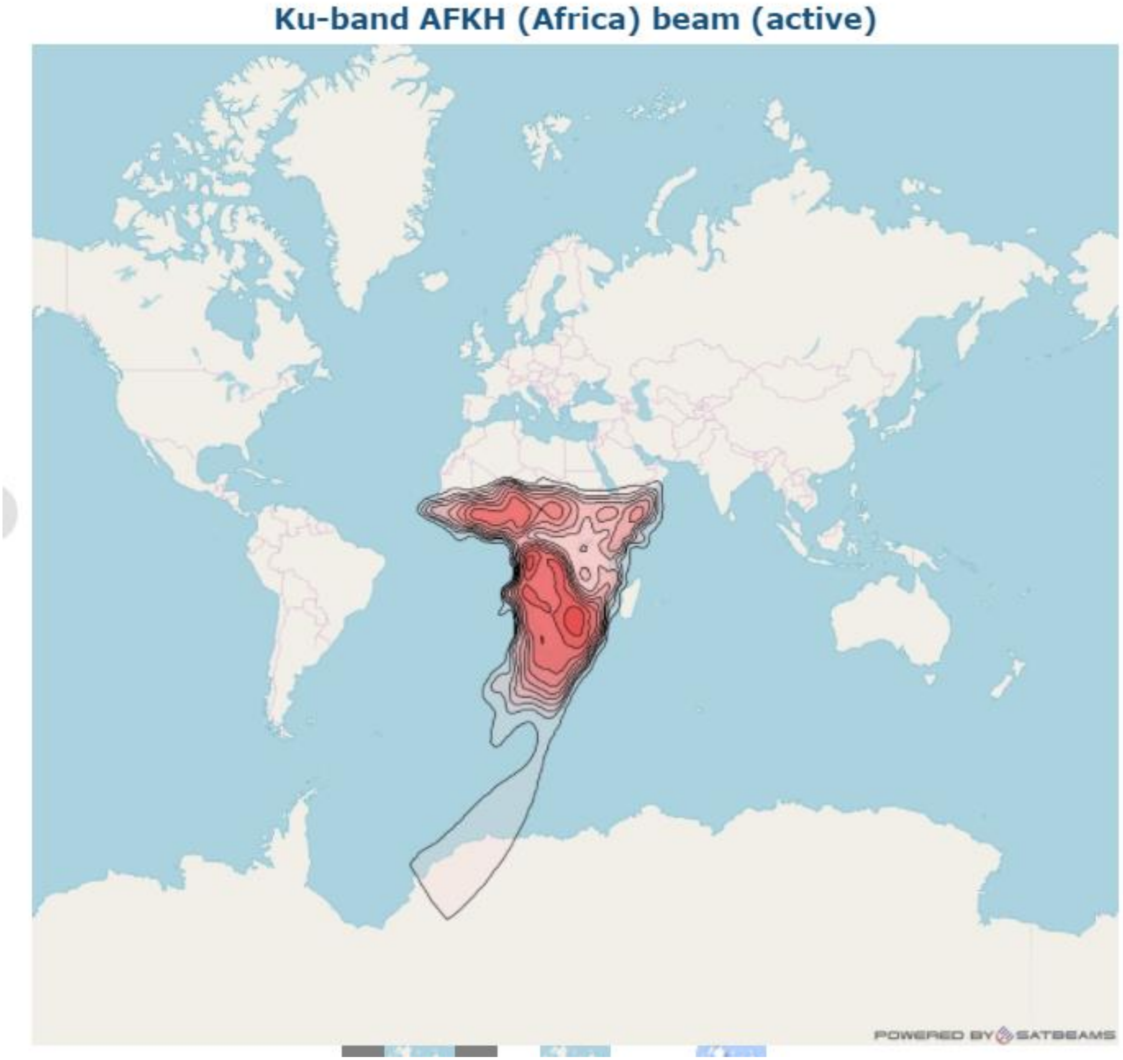
Ref: https://portswigger.net/

Threats & Impacts: Filings & Footprints





https://launiusr.files.wordpress.com/2014/12/geosynch-old.jpg



https://www.satbeams.com/

Threats & Impacts: Potential Loss

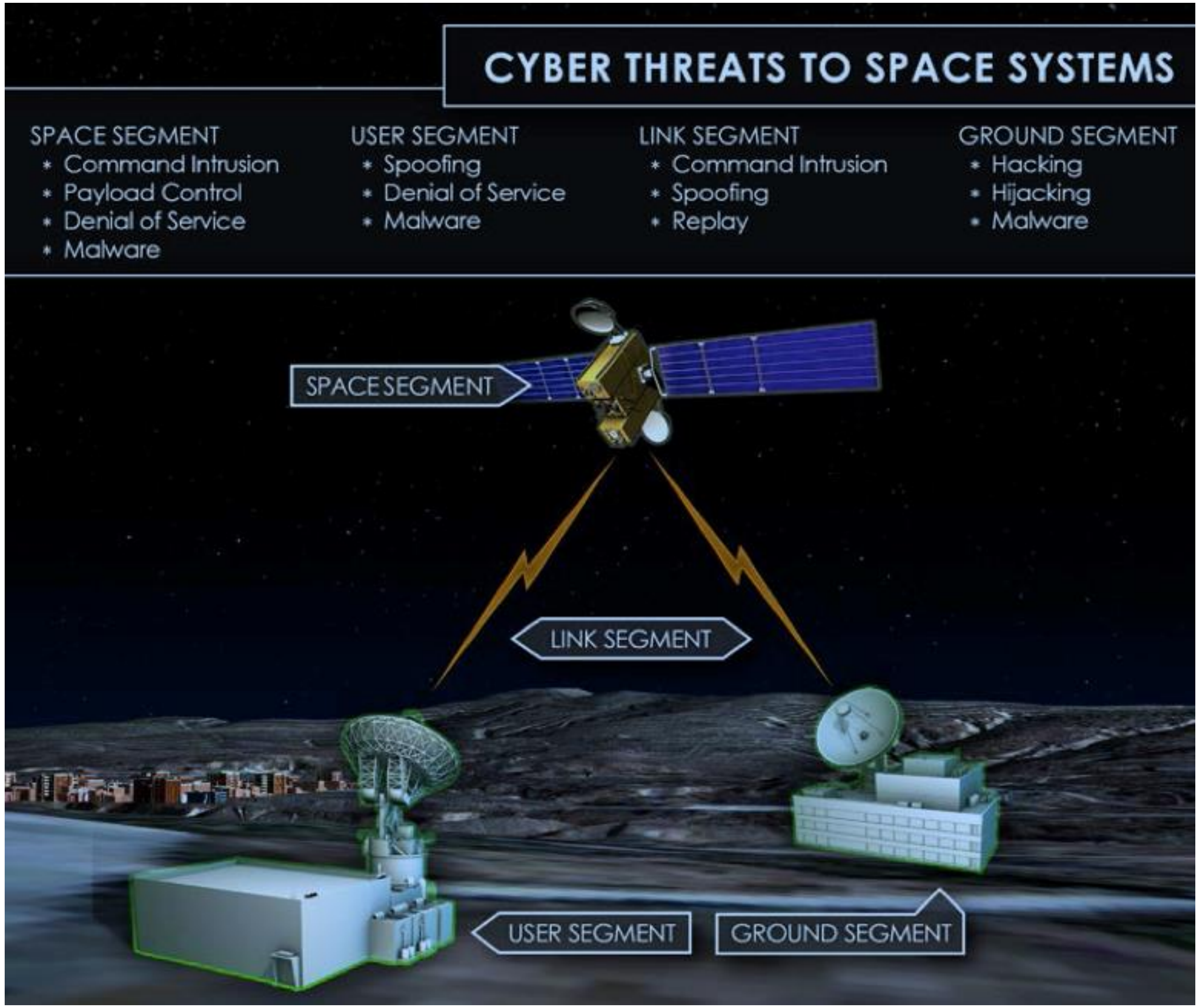
Space Mission Area	Potential Loss
Space Situational Awareness (SSA)	Space-based assets
Position Navigation Timing (PNT)	Precision targeting
Satellite Communication (SATCOM)	Tactical communications
Missile Warning	Response time
Environmental Modeling	Weather/Space Weather
Space-based Surveillance	Battlespace visibility

Cyber/related attacks on space capabilities (space, link, user, ground segments) should be viewed as part of adversary Anti-Access and Area Denial (A2/AD)

Cyber/related attacks on space capabilities should be viewed as part of campaign to contest the US Homeland

Where do we go from here?

- Map space & cyberspace interconnected **assets**
- Understand the **impacts/losses** if space capabilities are taken away by cyberattack
- Know that space systems are key **targets** by many families of threat actors
- Realize the concept of **contested environments** includes space & cyberspace



Ref: https://www.buffalo.edu/space-cybersecurity/center/why-space-cyber.html

Check out DEF CON 28 “Satellite Hacking” Talk: https://www.youtube.com/watch?v=ku0Q_Wey4K0&t=4s

Thank you, US Space Force: Cyber Expo 2021!

For the honor and privilege of this speaking opportunity!

Presentation(s) on GitHub: https://github.com/cyberguy514/presentations

Questions?

Contact Details:

Civilian: brhodes@zvelo.com

Military: brad.e.rhodes.mil@army.mil

MCPA: brad.rhodes@milcyber.org

LinkedIn: https://www.linkedin.com/in/brad-rhodes-1951ba7/

Twitter: @cyber514