CubeSat Developers Workshop 2025

Ethics + Emerging Sciences Group

DISCLAIMER

Ethics + Emerging Sciences Group

All statements are the author's alone and not of any organization, incl. Cal Poly, NASA. All images and copyrights are properties of their respective owners, per the "fair use" clause (US Code, Title 17, § 107

Thank You Pat Lin our leader on this project for including us and working so hard on this important topic!

Introductions

Ethics + Emerging Sciences Group

Bruce DeBruhl, PhD

Associate professor at Cal Poly, San Luis Obispo, in the Computer Science and Software Engineering Department, as well as the Computer Engineering Department. I am also an advanced computer scientist at SRI International, a non-profit research institute with strength in cybersecurity research, amongst other topics. Dr.DeBruhl works on both cybersecurity education and research in multiple domains.

Henry Danielson MA

Broad depth of knowledge in cybersecurity/computer/Satellites & Space Security research and obtained a Certified Information Systems Security Officer (CISSO). His current roles include serving as a technical advisor at the California Cybersecurity Institute (CCI), a lecturer at Cal Poly, San Luis Obispo for 21 years. Mr. Danielson is also a GOON at DEFCON. I am part of the Aerospace Village Team at DEFCON.

Context

Ethics + Emerging Sciences Group

- Briefing of Cal Poly's recent report
- Site: https://**space**cybersecurity.org
- US National Science Foundation SaTC award no. 2208458

- ICARUS = **I**magining **C**yberattacks to **A**nticipate **R**isks **U**nique to **S**pace

Ethics + Emerging Sciences Group

ICARUS Matrix & Outer Space Cybersecurity

Navigating the New Frontier: Addressing the Urgency of Outer Space Cyberattacks and Expanding Scenario Planning

CactusCon February 14-15 2025

Bruce DeBruhl, PhD, & Henry Danielson MA
California Polytechnic State University | San Luis Obispo

Outer Space & Cybersecurity

The wake-up call

Ethics + Emerging Sciences Group

- **Viasat** modems & routers hacked *an hour* before Russia's invasion of Ukraine in Feb 2022
- **Starlink** came to the rescue and were also targeted by Russia, but no successful hack for 2 years
- Russia: hacking our satellites is ***casus belli (cause for war)***

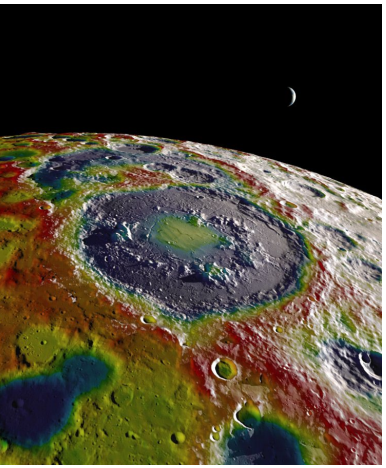
Space race 2.0

Ethics + Emerging Sciences Group

- Orbits are more **congested** and more **contested** than ever
- **Competition** for space resources and research sites
- Rise of **commercial** ventures without much governance
- Driven by technology, which is **hackable**

More conflict potential

Ethics + Emerging Sciences Group



- US and China are racing to set up bases on the **South Pole of the Moon**
- Nothing to prevent one from setting up a base **directly next to** others
- Inherently dangerous situation for competitors and **adversaries**
- **Legality** of safety zones and heritage sites is unclear

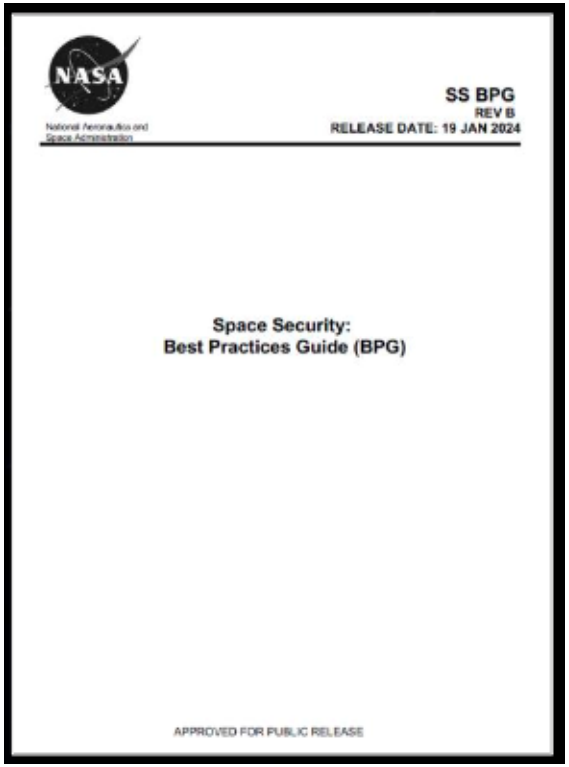
Ethics + Emerging Sciences Group

NASA Best Practices Guide

• Space Security Best Practices Guide (SS BPG), published in January 2024.
• Identifies SP800-53 controls relevant to space missions.
• Discusses 7 “Threat Actor Capabilities” referenced in Aerospace Technical Operating Report TOR-2021-01333:
• CAP-01: Ability to Access Networks
• CAP-02: Ability to Discover and Exploit Vulnerabilities
• CAP-03: Ability to Defeat Cryptography and Authentication
• CAP-04: Command and Control Sophistication
• CAP-05: Ability to Affect Cyber and/or Physical Systems
• CAP-06: Ability to Gain Physical Access
• CAP-07: Sophistication of Human Influence

• Analysis:
• This document contains some good framework ideas for how to organize the top-level cybersecurity
taxonomy, along with good cross-references to ATT&CK and SP800-53.

• Its “Mission Architecture Elements” provide good insight into how the cyber architectures for space elements
and ground elements should be different.


NASA
National Aeronautics and Space Administration

SS BPG
REV B
RELEASE DATE: 19 JAN 2024

Space Security:
Best Practices Guide (BPG)

APPROVED FOR PUBLIC RELEASE

Ethics + Emerging Sciences Group

NASA Best Practices Guide

- Also highlights 12 “MITRE ATT&CK Threat Actor Tactics:”
- TAC-01: Initial Access
- TAC-02: Execution
- TAC-03: Persistence
- TAC-04: Privilege Escalation
- TAC-05: Evasion
- TAC-06: Discovery
- TAC-07: Lateral Movement
- TAC-08: Collection
- TAC-09: Command and Control
- TAC-10: Inhibit Response Function
- TAC-11: Impair Process Control
- TAC-12: Impact

- Organizes protections into “three pillars” of design principles:
- PREVENT: remove the likelihood of cyber events
- MITIGATE: reduce the impact and/or likelihood of cyber events
- RECOVER: enable resiliency and restoration of capabilities impaired due to a cyber event

- Interestingly, this is a “Best Practices Guide” rather than “Formal Requirements.”

This document also divides mission areas into “Space Mission” and “Ground Mission” for the purposes of cyberdefense.

The usual suspects

Ethics + Emerging Sciences Group

Only a small handful of **vague** and **generic** scenarios typically gets trotted out, esp.:

- Something about satellite hacking
- Something about spoofing or jamming signals, such as GPS or military comms

….but there are *so many* more possibilities

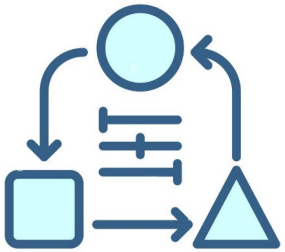
“Imagineering” scenarios

Ethics + Emerging Sciences Group

- **Failure to imagine** can be catastrophic, incl. not understanding different threat actors, motivations, vulnerabilities, etc.
- Humans are very creative and resourceful (when they want to be)
- Need to anticipate many more scenarios, to plan properly and **avoid surprises**
- Constant co-evolution of hunter and prey

Method to the madness

Ethics + Emerging Sciences Group



A. Threat actors (**who** is attacking?)
B. Motivations (**why** are they attacking?)
C. Attack methods (**how** would they do it?)
D. Victims (also related to the **who** question)
E. Capabilities affected (**what's** the effect?)

Note: the **when** and **where** depend on the scenarios and therefore aren't variables for our purposes

HackaSat

Ethics + Emerging Sciences Group

https://hackasat.com/learn/

SPACE GRAND CHALLENGE

Ethics + Emerging Sciences Group

https://cci.calpoly.edu/empower/space-grand-challenge-program

1802 Registrations for Middle and high school student competitors	**30** Cal Poly students developed managed the game and events	**497** 2024 Sandbox Hours Played
130 Game based challenges across 10 individual Unity game rooms	9 Countries 17 States	**1000+** Viewers have watched the broadcast, YouTube walkthroughs, and expert interviews.

Imagineering scenarios

Bruce

The ICARUS Matrix

Ethics + Emerging Sciences Group

	A: Threat actors	B: Motivations	C: Cyberattack methods	D: Victims / stakeholders	E: Space capabilities affected
1	Major space-faring states	Nationalism	Insider attack	Major space-faring states	GPS / GNSS
2	Other space-faring states	Dominance / influence	Social engineering	Other space-faring states	Earth observation / remote sensing
3	Non-space-faring states	Financial / economic	Ransomware	Non-space-faring states	Military intelligence and capabilities
4	Insider threats	Fraud	Honeypot	State-owned entities	Spacecraft, robotic or crewed
5	Political terrorists	Employment	Sensor attack	Military and other contractors	Life-sustaining services
6	Mercenaries	Blackmail / coercion	Signals jamming	Scientific organizations	Other essential services
7	Eco-terrorists	Terror	Signals spoofing or hijacking	Corporations	Other safety of personnel / others
8	Corporations	Warfare	Eavesdrop / man-in-the-middle	Wealthy individuals	Loss of sovereignty / control
9	Mobile service providers	Disinformation	Network security	General population / society	Earthbound services
10	Launch service providers	Espionage	Supply chain, hardware	Indirect / secondary stakeholders	Emergency services
11	Social engineering groups	Sabotage	Supply chain, software	Marginalized populations	Financial transactions
12	Organized crime	Extremist ideology	AI / ML / computer vision	Social movements	Mining or manufacturing
13	Chaos agents	Cult of personality	Attack coverup	Cultural / religious groups	Scientific capability / research
14	Religious / apocalyptic	Paranoia / anti-technology	Software hacking	Unions / labor reps	Asteroid detection systems
	Other ideological groups	dom / trolling	Systems	Customers / u their data	Space weather monitorin

On taxonomies

Ethics + Emerging Sciences Group

- ICARUS matrix is well suited for **simulation** or tabletop exercises
- Help to methodically **explore** a domain
- Existing taxonomies weren't the right fit
  - Too technical or detailed
  - Too general or simplistic
  - They address the *how*, but not *5 W's*

On scenarios

Ethics + Emerging Sciences Group

- **4+ million** prompts possible
- Not all combos make sense—that's a **feature**, not a bug
- 42 scenarios as a starting set
  - Organized by time x distance
  - Very brief for customization
- Humans are **hardwired** for stories—bringing invisible threats to life

Ex. 1: Eco-terrorists

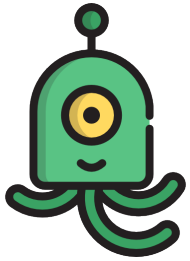
Ethics + Emerging Sciences Group

- Threat actor: motivated by a desire to **protect** the environment, either Earth or space; or to **harm** the environment for various reasons
- Goal: to allow a serious **wildfire** to continue burning by disrupting disaster tracking and response
- Target: key Earth observation **satellites**
- Method: **sensor/optical attack** primarily

Ex. 2: Religious cult

Ethics + Emerging Sciences Group

- Threat actor: perceives a decline in **religiosity** and wants to create a seismic event that forces people to seek out religion
- Goal: to spoof a **technosignature** (evidence of ET life) in hopes of creating global panic
- Target: **James Webb Space Telescope**
- Method: **injects false data** in the downlink to Earth



Ex. 3: Bored teenager

Ethics + Emerging Sciences Group

- Threat actor: motivated by **idle curiosity** to see if a certain hack could be done
- Goal: to **deorbit** a university aerospace project…which accidentally causes collisions and creates orbital debris
- Target: **CubeSat** with prototype *thrusters*
- Method: **insider attack**, in stealing roommate's credentials to inject a bad command in uplink

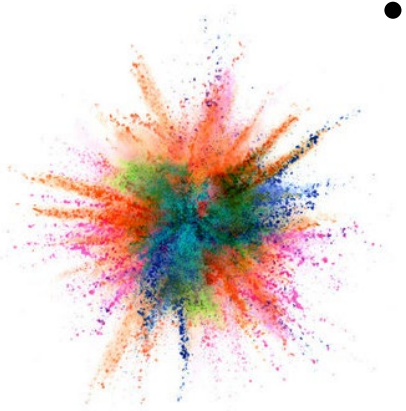
Ex. 4: Industry rivals

Ethics + Emerging Sciences Group

- Threat actor: an aggressive, **maverick** company, looking for a competitive edge
- Goal: to **sabotage** a competitor's space hotel (before it opens) to scare away investors, customers
- Target: **life-support systems**, e.g., air, water, food, etc.
- Method: **supply-chain hack**, as both companies share suppliers

Bringing threats to life

Ethics + Emerging Sciences Group



- Compare these scenarios to the usual **vague** ones about “hacking a satellite” or “spoofing signals”
- Details can **inform** security planning
  - **Clearer** targets to aim at
  - Different scenarios can suggest **different defenses** and **response-options**

Closing thoughts

Key points

Ethics + Emerging Sciences Group

- Space is a **critical domain** to defend
- Cyberattacks as the **primary mode** of conflict, esp. to avoid more orbital debris
- Threat environment is constantly **evolving**
- Essential to **understand** threat actors, motivations, as well as space system vulnerabilities and capabilities
  - Need to team up with **diverse experts**

The nature of frontiers

Ethics + Emerging Sciences Group

"Outer space is the next **frontier** for cybersecurity. To guard against space cyberattacks, we need to understand and anticipate them, and **imagination** is at the very heart of both **cybersecurity** and **frontiers**."

— Cal Poly report

Acknowledgements

Ethics + Emerging Sciences Group

- This work is supported by the **US National Science Foundation**, grant no. 2208458
- Also: **Cal Poly,** College of Liberal Arts and Philosophy Dept.
- Opinions are the author's alone and not of any of the orgs mentioned here

- All images/copyrights are properties of their respective owners, per the "fair use" clause (US Code, Title 17, §107)

LEARN BY DOING

Thank you!

Ethics + Emerging Sciences Group

Dr. Bruce DeBruhl
bdebruhl@calpoly.edu

Henry Danielson
hdaniels@calpoly.edu

Appendix: **ICARUS Matrix**

	A: Threat actors	B: Motivations	C: Cyberattack methods	D: Victims / stakeholders	E: Space capabilities affected
1	Major space-faring states	Nationalism	Insider attack	Major space-faring states	GPS / GNSS
2	Other space-faring states	Dominance / influence	Social engineering	Other space-faring states	Earth observation / remote sensing
3	Non-space-faring states	Financial / economic	Ransomware	Non-space-faring states	Military intelligence and capabilities
4	Insider threats	Fraud	Honeypot	State-owned entities	Spacecraft, robotic or crewed
5	Political terrorists	Employment	Sensor attack	Military and other contractors	Life-sustaining services
6	Mercenaries	Blackmail / coercion	Signals jamming	Scientific organizations	Other essential services
7	Eco-terrorists	Terror	Signals spoofing or hijacking	Corporations	Other safety of personnel / others
8	Corporations	Warfare	Eavesdrop / man-in-the-middle	Wealthy individuals	Loss of sovereignty / control
9	Mobile service providers	Disinformation	Network security	General population / society	Earthbound services
10	Launch service providers	Espionage	Supply chain, hardware	Indirect / secondary stakeholders	Emergency services
11	Social engineering groups	Sabotage	Supply chain, software	Marginalized populations	Financial transactions
12	Organized crime	Extremist ideology	AI / ML / computer vision	Social movements	Mining or manufacturing
13	Chaos agents	Cult of personality	Attack coverup	Cultural / religious groups	Scientific capability / research
14	Religious / apocalyptic	Paranoia / anti-technology	Software hacking	Unions / labor reps	Asteroid detection systems
15	Other ideological groups	Boredom / trolling	Systems security	Customers / users via their data	Space weather monitoring
16	Proxies / agents, esp. unwilling	See world burn / chaos	Multi-phase attack / APT	Individual targets	Space traffic management
17	Noncombatants, esp. unwilling	Social / distributive justice	Cloud hacking	Critical specialists	Space tourism
18	Amateur hackers / enthusiasts	Intellectual / tech demo	Account compromise	Critical infrastructure	Launch capabilities
19	AI / machine learning	Revenge / retaliation	Quantum computing / comms	Internet / media / entertainment	Communications
20	Unknown / anonymous	First contact, for and against	Death by 1,000 cuts / long game	AI / machine learning	News / social media