2021 13th International Conference on Cyber Conflict
Going Viral
T. Jančárková, L. Lindström, G. Visky, P. Zotz (Eds.)
2021 © NATO CCDCOE Publications, Tallinn

In the Same Boat: On Small Satellites, Big Rockets, and Cyber Trust

James Pavur
University of Oxford
Department of Computer Science
Oxford, United Kingdom
james.pavur@cs.ox.ac.uk

Martin Strohmeier
armasuisse
Science + Technology
Thun, Switzerland
martin.strohmeier@armasuisse.ch

Vincent Lenders
armasuisse
Science + Technology
Thun, Switzerland
vincent.lenders@armasuisse.ch

Ivan Martinovic
University of Oxford
Department of Computer Science
Oxford, United Kingdom
ivan.martinovic@cs.ox.ac.uk

Abstract: Launch vehicle "ridesharing" has redefined access to and use of outer space. Today, rockets carry satellites from dozens of countries on shared journeys towards the stars. To ensure that these diverse payloads pose no threat to the overall space mission, safety controls have emerged to protect against mechanical and electrical failure. While these protections were designed to mitigate the risk of probabilistic physical effects, they also have implications for cyber attackers seeking to abuse the trusted status of secondary payloads to harm launch missions.

This paper considers such dynamics through a multidisciplinary lens. It begins by drawing on the perspective of security studies and international relations to characterize what motivates an attacker to target satellite launches. This is combined with a technical analysis which leverages model-based engineering techniques to assess the threat of electronic warfare (EW) and radio frequency interference (RFI) attacks against missile range safety technologies on modern launch vehicles. Through dynamic physical simulation, we demonstrate that even inexpensive nanosatellite platforms have the potential to threaten shared launch vehicles in the hands of motivated cyber adversaries. The paper concludes with a brief discussion

of the implications of these findings for both policymakers and technical researchers interested in cyber-physical threats in orbit.

Keywords: *space, ASAT, threat modeling, cyber-physical, aerospace, critical infrastructure*

1. INTRODUCTION

The emergence of small, low-cost secondary satellite payloads, referred to as CubeSats, has underpinned a revolution in modern space mission design. This has, in turn, reshaped the satellite launch market. Where in the past, rockets carried hardware belonging to a single nation-state or a handful of domestic organizations, today a single launch vehicle may take satellites belonging to dozens of foreign entities on a shared ride to the stars. In this paper, we consider how these trends intersect with the evolving domain of space cyber security.

We take an interdisciplinary approach, starting with an analysis of the global CubeSat launch market and relevant interstate political dynamics. This motivates a novel threat model, leveraging CubeSat payloads as cyber-physical attack vectors against launch operations. We isolate five key CubeSat safety standards which may constrain cyber adversaries but find that most operate under trust assumptions which are vulnerable to malicious circumvention.

Rather than restricting ourselves to high-level strategic threat modeling, we cultivate a baseline intuition for the implications of such malicious safety violations through dynamic physical simulations of a space-to-space radio frequency interference (RFI) attack scenario. The results of these simulations suggest that, even when limited to standard CubeSat components, attackers have wide physical margins within which to cause sustained intentional degradation to safety-critical communications during launch.

This research makes several contributions presenting a novel analysis at the intersection between "launch diplomacy," hardware safety, and cyber security. It represents one of the first attempts to consider the cyber security properties of space launches and, to our knowledge, the first publication to consider space-to-space cyber warfare operations from secondary payloads as a threat vector. Methodologically, this paper demonstrates how policy analysis, model-based engineering methods, and system security techniques can combine to provide cross-domain insights into emerging threats. Finally, the case study, which makes up the latter portion of the paper, serves

as a cautionary example of how safety engineering controls are not necessarily robust to intelligent and strategic adversaries.

2. BACKGROUND

A. CubeSats and Ridesharing

Orbital access is expensive. Even with state-of-the-art technology, single rocket launches can exceed hundreds of millions of dollars (see Table I). To overcome this barrier, satellite owners engage in "ridesharing," purchasing excess capacity on someone else's launch vehicle (LV) for a secondary payload.

TABLE I: EXAMPLE PER-LAUNCH COSTS AND CAPABILITIES OF MODERN LVS

Vehicle	Approx. Launch Cost (USD)	Approx. Mass-to-Orbit (t)
Ariane 5 (ESA)	$150 million [1]	10 (GTO) – 20 (LEO)
Delta IV (NASA)	$300 million [2]	14 (GTO) – 29 (LEO)
Falcon 9 (SpaceX)	$60–100 million [3]	8 (GTO) – 23 (LEO)

Note: GTO = Geosynchronous Transfer Orbit, LEO = Low Earth Orbit

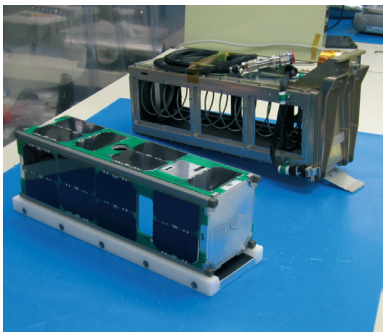
Ridesharing practice has co-evolved with a satellite design template, referred to as CubeSats [4]. CubeSats are small and lightweight, with the smallest size (1 CubeSat Unit or 1U) only 10 cm^3 in volume and weighing approximately 1.3 kg. For missions which require large components, multiple 1U cubes can be combined. For example, a 30 × 10 × 10 cm payload weighing around 4 kg would be referred to as a 3U CubeSat.

Compared to traditional satellites, CubeSats are small and cheap, with complete mission costs ranging from tens of thousands to a few million euros [5]. Readymade CubeSat platforms can be purchased online for as little as 25,000 euros, although most missions will require some additional customization [6]. This has made CubeSats the platform of choice for many space start-ups and research missions.

The standard shape and mass of CubeSats allows for easy integration to LVs via standardized deployers, thereby creating a sort of commodity market for global CubeSat launch capacity. The dominant deployer type is the P-Pod (see Figure 1) [4]. A P-Pod is essentially an aluminum box with a door on one end and a spring on the other. When the door's latch is released by the LV flight computer, the spring ejects

up to 3U of CubeSats into space at a velocity of 1–2 m/s. Other deployer types tend to follow similar design principles [7], [8].

FIGURE 1: A 3U CUBESAT (FRONT) AND P-POD (BACK) [9]



The global rocket launch market to deliver such payloads is consolidated into a handful of major players. Between 2016 and 2019, 90% of the estimated 29 billion US dollars spent on launch services went to one of seven space powers: United States, European Union, China, Russia, Japan, India, and New Zealand [10]. The content of these missions, on the other hand, is highly internationalized. For example, the European Space Agency (ESA) Vega SSMS mission in 2020 delivered a total of 53 satellites to Low Earth Orbit (LEO) [11]. These included platforms for the Thai military, a Russian nuclear physics institute, an Estonian university, and a Facebook subsidiary. In total, 21 customers from 13 countries shared the same journey to the stars.

B. Space Diplomacy and Ridesharing

These multi-state missions occur against a complex geopolitical backdrop. LVs have been longstanding subjects of tension due to their dual-use potential; other than the direction they face, and the logo painted on their side, there is little differentiating an LV from an intercontinental ballistic missile (ICBM). Indeed, both the US and Russia regularly repurpose retired ICBMs for space launches, and responses to North Korea's domestic space program have been inextricably linked to arms control concerns [12]–[14].

The tensions do not stop at the atmosphere's edge. Major military powers rely heavily on space for battlefield communications and operations. As satellites are physically fragile, there is significant fear of attacks on space assets in future conflicts [15]. In particular, prior research has argued that states have strong incentives to engage in cyber attacks due to structural advantages favoring cyber attackers in the space domain [16].

However, there have also been many indications of interstate cooperation. Throughout the Cold War, significant efforts were made by both the US and USSR to cooperate on space launches, giving rise to the Apollo-Soyuz Test Project (ASTP). It has been argued that "track II diplomacy" resulting from interpersonal relationships cultivated during ASTP gave rise to broader diplomatic gains, such as strategic arms control agreements and the demilitarization of Russia's launch sector [17]. In a more modern context, launch collaboration for the International Space Station (ISS) was one of the few aspects of the US-Russia bilateral relationship to survive the diplomatic fallout of Russia's invasion of Crimea in 2014 [18].

Some classical realists treat this sort of cooperation with skepticism. For example, Wang's review of US-EU space cooperation argues that the US used LV ridesharing as a tool to undermine and weaken European rocketry development efforts [19]. Likewise, Chalecki contends that the ASTP was little more than a guise for the US and Soviet military intelligence to spy on each other [20].

In short, satellite ridesharing is as much a geopolitical matter as a technical one. Ridesharing offers direct economic benefits, but it also redirects huge sums of money into foreign aerospace industries and provides political leverage to LV operators that may be unpalatable to some satellite owners.

3. THREAT MODELING

In this context, we can surmise several motivations for cyber attackers to target launches. A launch failure could prevent or delay the deployment of key space assets. Moreover, commercial actors may see a benefit in harming the reputation of key competitors. For example, this was briefly investigated as a possible cause of a 2016 SpaceX rocket explosion [21]. The prestige and economic importance of space programs may also make them attractive targets for hostile states – as Russian officials suggested following a string of rocket failures in the early 2010s [22], [23].

For this paper, we focus on threats involving the compromise of an inexpensive CubeSat secondary payload. We propose four reasons CubeSats may represent attractive targets.

1) Heavy use of commercial-off-the-shelf (COTS) components allows attackers to develop exploits on representative hardware or software. This contrasts with larger platforms which tend to rely on bespoke components.

2) The COTS supply chain can be compromised; for example, through a backdoor in an open-source software library or the online sale of a malicious sensor. The high number of CubeSats per LV increases the odds of a backdoored product ending up attached to an LV of interest to an attacker.
3) While large satellites and LVs are typically built by nation-states and defense contractors, CubeSats frequently come from start-ups or universities. These organizations are comparatively permeable to digital compromise, insider threats, sabotage, and social engineering.
4) CubeSats are inexpensive. Combined with the pseudo-commodity market for CubeSat launch slots, a proxy corporation or state-sponsored university could afford many attempts at building and launching a CubeSat with malicious flight software that abuses trusted/approved COTS components to cause harm.

To date, little prior technical research exists on CubeSat cyber security in large part due to their low capabilities and small size. To quote one CubeSat developer: "What's the worst that could happen? […] With no propulsion and no pointing control, it's very likely that you couldn't do anything other than turn the camera off" [24]. CubeSat manufacturers have lobbied against cyber-security standards, contending that they pose "an excessive and unnecessary burden, and a major potential mission-reliability risk" [24]. The effect of this mentality is that CubeSats tend to forgo security to meet aggressive cost and schedule requirements. Additionally, in a high-level review of CubeSat security practices, Ingols and Skowyra note that CubeSat developers will often "conflate reliability engineering with security engineering" [25, p. 11].

This is an important point, because while security risks are frequently dismissed, attackers may still struggle to cause meaningful harm after successfully compromising a CubeSat. CubeSats represent many organizations' first space mission and, as a result, often fail. Roughly 50% of CubeSats suffer "infant mortality," failing within six months, and one in five are "dead on arrival," never making contact with Earth at all [26], [27]. Launch providers are thus keenly aware of the risks of strapping unreliable novice hardware, however small, to a cylinder full of rocket fuel. This has given rise to extensive controls designed to limit the mechanical and electrical risk a CubeSat can pose to the LV. In Section 4, we will consider these safety controls and their implications for an intelligent cyber adversary.

4. ADVERSARIAL ANALYSIS OF LAUNCH SAFETY CONTROLS

CubeSat safety requirements can vary substantially and revolve around a series of mission-specific Interface Control Documents (ICDs) provided by the mission integrator. These requirements are complex and certification is non-trivial; NASA recommends allowing 18 months for certification and licensing [28]. In this paper, we focus on two dominant standard documents (among myriad) for CubeSat missions: the *CubeSat Design Specification, REV 13* (CDS) and the *Air Force Space Command Manual 91-710, Volume 3* (AFSPCMAN) [29], [30].

A. CubeSat Design Specification (CDS)

The CDS focuses mostly on the physical properties which may impact a CubeSat's ability to deploy smoothly from a P-Pod. Beyond this, it imposes three broad categories of controls which appear to constrain cyber adversaries.

First, CDS requires deployment switches, small pins on CubeSat rails which are depressed while the CubeSat sits in its P-Pod [29, Sec. 3.3]. These electrically isolate the CubeSat's flight computer from power during launch to prevent a CubeSat from deploying hardware in the P-Pod. They also prevent attackers from launching software-based attacks prior to deployment. Second, CDS prohibits CubeSats from transmitting radio signals until 45 minutes have elapsed from deployment, although the CubeSat may boot up and perform other tasks in that time [29, Sec. 3.4]. This mitigates the risk of both unintentional and malicious radio frequency interference (RFI). Third, CDS typically limits stored chemical energy to 100 watt-hours [29, Sec. 3.1]. This limits the available power for direct physical harm – such as deliberate overheating of key components.

These controls are normally verified using three mechanisms [28]. Battery characteristics are outlined in a battery report, which details specific part numbers and modifications. Radio and electrical interrupts are summarized in an electrical report containing circuit diagrams. Finally, inhibits are verified during a Day in the Life (DITL) test. In a DITL, the CubeSat runs through a simulated separation and a timer is used to verify that no premature transmissions take place. The DITL is typically conducted by the CubeSat developer in their own lab [31], [32].

B. Air Force Space Command Manual 91-710 (AFSPCMAN)

AFSPCMAN consists of more than 200 pages of requirements for launch operations, the primary purpose of which is range safety. The objective of range safety is to protect individuals, vehicles, and structures from harm and ensure that rockets adhere to intended trajectories. Range safety violations can result in the initiation of a self-

destruction system known as a Flight Termination System (FTS), which is designed to ensure that a launch vehicle combusts fully prior to colliding with the Earth's surface.

The primary AFSPCMAN burden for CubeSat developers is the provision of a Missile System Prelaunch Safety Package (MSPSP), prepared by the CubeSat developer [30, p. 214]. It consists of a detailed description, including schematics and functional diagrams, of the payload and relevant hazards.

The most obviously applicable portion of AFSPCMAN to cyber security is the portion on Computer Systems and Software [30, p. 200]. Software security requirements are derived from Software Criticality Indexes (SwCIs) specified in MIL-STD-882E [33]. A synthesis of these requirements can be found in Table II. In most cases, CubeSat software falls in the range of SwCI 4-5, with DITL testing meeting validation burdens. The only additional software safety hurdle is likely a descriptive overview of computing hardware components and software logic [34].

TABLE II: OVERVIEW OF AFSPCMAN SOFTWARE SAFETY STANDARDS

	Severity Level of Safety Failure			
Software Control Category	**Catastrophic** *(e.g., loss of life, > $10M damages)*	**Critical** *(e.g., hospitalization of 3+ personnel, > $1M damages)*	**Marginal** *(e.g., injury causing lost workdays, > $100K damages)*	**Negligible** *(e.g., minor injury, < $100K damages)*
Autonomous	SwCI 1 (Code Review)	SwCI 1 (Code Review)	SwCI 3 (Architecture Review)	SwCI 4 (Safety-Specific Testing)
Semi-Autonomous	SwCI 1 (Code Review)	SwCI 2 (Design Review)	SwCI 3 (Architecture Review)	SwCI 4 (Safety-Specific Testing)
Redundant Fault Tolerant	SwCI 2 (Design Review)	SwCI 3 (Architecture Review)	SwCI 4 (Safety-Specific Testing)	SwCI 4 (Safety-Specific Testing)
Influential / Informational	SwCI 3 (Architecture Review)	SwCI 4 (Safety-Specific Testing)	SwCI 4 (Safety-Specific Testing)	SwCI 4 (Safety-Specific Testing)
No Safety Impact	SwCI 5 (No Analysis)	SwCI 5 (No Analysis)	SwCI 5 (No Analysis)	SwCI 5 (No Analysis)

Note: The controls in this table are synthesized from multiple tables in *MIL-STD-882E* and controls in *AFSPCMAN 91-703v3* [30], [33]. All controls which apply to lower severity Software Criticality Indexes (SwCI) apply to high severity indexes cumulatively.

Beyond software safety, the MSPSP also imposes requirements to mitigate the risk of electromagnetic interference. A CubeSat developer typically must provide a transmitter survey, which lists all radio transmitters and their fundamental characteristics. This includes an outline of frequency ranges, bandwidth, and deployed and maximum power delivery to a given antenna [28].

Range safety may require verification of emission characteristics through measurements conducted by an approved representative [30, p. 43]. However, in practice, CubeSat missions may be able to avoid the costs and scrutiny of such assessment through the use of RF power inhibits [34]. If frequency analysis is required, the main purpose is to ensure that payload emissions do not broadcast on key frequencies outlined in the LV's specification. These frequencies are often listed in public documentation and typically consist of telemetry and FTS modules [35], [36].

C. Adversarial Analysis

Initially, these controls appear to severely constrain an attacker's capabilities. However, their implementation assumes an informed and benign CubeSat developer who shares the launch integrator's desire for a successful mission.

Under our adversarial model, this shared priority does not exist. CubeSat developers may be unaware of or complicit in efforts to circumvent controls. As large parts of the certification process are self-reported, violating controls is often little more than a matter of ticking an incorrect box or writing down inaccurate numbers on a form. Attackers can strategically evade only a small subset of the hundreds of standards, maximizing potential harm while minimizing detectability.

For example, Ingols and Skowyra note that CubeSats spend the months between completion and launch being passed around different storage facilities and may be subject to post-certification tampering via social engineering vectors [25]. A sophisticated attacker may make minor software modifications to devices during this time with little risk of detection. Even more severely, if the CubeSat developer misrepresents DITL results or electrical diagrams, there is no clear mechanism for detecting this; CubeSats are too fragile to disassemble for manual inspection.

These deceptions may be intentional, or they may come from further up the supply chain. A malicious COTS vendor, for instance, might provide a telemetry module which they purport to broadcast in certain launch compatible frequencies when, in fact, a hidden backdoor enables transmissions in prohibited bands or power levels.

In Table III, we present a demonstrative analysis of five controls from CDS and AFSPCMAN under adversarial conditions. These controls were selected as likely

targets for attackers seeking to cause cyber kinetic harm within the constraints of CubeSat hardware. For each, we note the source of verification authority and deception exposure to both insiders and outsiders.

TABLE III: ADVERSARIAL CIRCUMVENTION ANALYSIS FOR SELECTED SAFETY CONTROLS

Safety Control	Primary Reference	Responsible for Verification	Likely Vulnerability to Malicious Outsider	Likely Vulnerability to Malicious Insider
Deployment switches prevent power-on in deployer	CDS 3.3	CubeSat Developer (DITL, Electrical Diagrams)	**Low** *CubeSat developer would likely detect unauthorized power draw during DITL.*	**High** *CubeSat developer could forge documentation and DITL results.*
Software timers prevent RF transmission for 45 minutes	CDS 3.4	CubeSat Developer (DITL)	**Moderate to High** *Otherwise trivial modifications to code may necessitate special effort to evade DITL detection.*	**High** *CubeSat developer could forge DITL results or program DITL behavior to differ from launch.*
Battery power limitation	CDS 3.1	CubeSat Developer (Battery Report, MSPSP)	**Low** *Malicious vendor could misrepresent battery specs but targeting is logistically complex.*	**Low to Moderate** *Weight and physical properties act as limits on plausible extent of deception.*
Software Safety Guidance	AFSPCMAN A2.2.4.14	CubeSat Developer (MSPSP)	**High** *Software, especially third-party libraries, is unlikely to be audited beyond cursory summary in MSPSP.*	**High** *CubeSat developer will likely only need to provide easily falsified summary information on software operations and design.*
RF Emission Compatibility	AFSPCMAN A2.2.4.10.2, Launch Vehicle User's Guide	CubeSat Developer (MSPSP) Range Safety (EMF testing)	**Low to Moderate** *Malicious vendor could backdoor telemetry hardware. If a software defined radio (SDR) is used, attacker may modify configuration using code.*	**Moderate to High** *In the absence of independent EMF testing, CubeSat developer can lie. Otherwise, they may modify code to change behavior under test conditions.*

This analysis suggests that many of the controls which help ensure safety during the CubeSat integration process are not robust to an intelligent adversary. For example, requiring triple-redundant radio inhibits (CDS 3.4) dramatically reduces the risk from equipment failure. However, there is little difference from the perspective of a malicious CubeSat developer lying once in their electrical report versus lying thrice. Even absent insider access, the lack of software and supply-chain auditing processes provides ample opportunity for cyber attackers to circumvent key safety requirements.

5. THREAT SIMULATION AND EVALUATION

Given the common perceptions that a CubeSat's low capabilities mean that, even in the event of full compromise, it cannot pose a physical threat, it is worth considering the specific technical implications of malicious safety control violations. To do this, we will replicate a hypothetical attack scenario through dynamic physical simulation. The intent is not to completely model the behavior of LVs and satellites but rather to evaluate the general plausibility of harm from compromised CubeSat hardware during launch.

Our hypothetical threat scenario focuses on GPS interference attacks for three reasons. First, RFI attacks are intuitively bolstered by physical proximity – one of the main boons from compromising a secondary payload. Second, what limited public information is available on LV FTS hardware makes it clear that GPS is a key data source [37]. Finally, due to US commercial radio licensing regulations, there is a relative abundance of technical data regarding representative radio hardware, helping to better ground our simulations [38].

A. Scenario Overview

The compromised CubeSat in our simulation is summarized in Table IV. It consists of a notional 3U commercial payload, weighing 4 kg and scheduled for launch on a SpaceX Falcon Heavy. The mission sequence is loosely modeled on that of the STP-2 launch. STP-2 is selected as an example of a mission which deployed CubeSats *en route* to delivery of the primary payload. This emerging practice offers commercial and logistical benefits, but also raises the risks from compromise as CubeSats are deployed while the primary payload and substantial fuel quantities remain in the LV.

Our attacker is derived from the insider model in the rightmost column of Table III. It is a malicious state-sponsored business that has built a CubeSat with the express purpose of circumventing key safety controls. To reduce scrutiny, the attacker is restricted to standard CubeSat components. There are two relevant hardware modules used in the attack, both belonging to the CubeSat's Telemetry, Tracking and Control (TT&C) subsystem.

First, the CubeSat leverages a software defined radio (SDR) transceiver. Specifically, we have modeled our simulation around the 1U μSDR-C from Space Micro [39]. An SDR permits the attacker to dynamically alter radio transmission parameters, including carrier frequencies, using undisclosed software logic. SDRs are commonly used in CubeSats and the presence of an on-board SDR alone would be unlikely to arouse suspicion. Additionally, the attacker has selected an antenna with undisclosed operability in the 1.1–1.6 GHz range as well as the allocated TT&C band. This can

be achieved with a customized deployable antenna, a multi-band module, or an ultra-wideband offering [40]–[42]. This frequency range is selected due to its potential to cause interference with GPS reception.

TABLE IV: ATTACKER CUBESAT CHARACTERISTICS AND OBJECTIVES

Size & Weight	Relevant RF Range	Attacker RF Tx Power	Attacker Objective	Targeted Frequencies	Effective Power at LV
3U, 4 kg	1.1–1.6 GHz	1–10 W	Interfere with L-Band GNSS reception on launch vehicle	1575.42 MHz (GPS Rx)	Approx. -120 dBm (Rx) [43]

The attacker has also inserted malicious programming logic with the intention of circumventing two safety controls from Table III. First, the attacker will begin RF transmission immediately after separation from the P-Pod, violating the 45-minute silence mandate. Second, the attacker will transmit on frequencies prohibited by AFSPCMAN A2.2.4.10.2 and the Falcon User's Guide [35]. To evade detection during lab certification and DITL tests, this malicious logic will check the measurements of on-board sensors (e.g., a thermometer) and only trigger the attack when conditions match LEO.

The attacker's goal is to introduce RFI of sufficient magnitude to trigger a range safety incident on the LV. For example, if positional telemetry data is unavailable or indicates a rocket has strayed from its intended trajectory, this can lead to a mission abort.

This is particularly relevant for the Falcon Heavy, as it is one of the first LVs to include a fully autonomous flight termination system (AFTS) [35, p. 8]. This AFTS can automatically self-destruct the launch vehicle without human approval if sensors show a deviation from approved mission parameters. Although the precise AFTS specifications are, unsurprisingly, restricted, NASA documents confirm GPS observations as a key decision metric for termination [37].

B. Experimental Design and Assumptions

The primary purpose of these simulations is to determine the plausible limits of CubeSat hardware to emit an RF signal which causes sustained degradation to GPS reception. In practice, many relevant dynamics are mission-dependent, such as antenna directionality, GPS satellite locations, and precise launch trajectories. Here, we focus on a "worst case" scenario based on typical GPS signal characteristics, idealized isotropic antennas, and the assumption of equivalent receiver gain across legitimate and illegitimate transmission sources.

1) Model Parameters

According to the Falcon User's Guide, the launch vehicle contains GPS receivers which operate in the L1 signal band (1574.2 MHz) [35]. To determine the necessary jammer characteristics to cause disruption to these signals, we must approximate the strength of legitimate signals at the receiver. The GPS specification only provides information regarding the Earth's surface, but we can derive a more accurate value for LEO. One method for doing so is presented in [43], suggesting an approximate received power of around -120 dBm in dynamic simulation. This is fairly close to the value predicted by a simple Free Space Path Loss (FSPL) model on the basis of the public GPS L1 link budget – with minor modification to account for LEO conditions (see Equations 1–3) [44].

Letting:

$$FSPL(dB) = -10 \times \log_{10}\left[\left(\frac{4\pi d}{\lambda}\right)^2\right] \tag{1}$$

and:

$$P_{rcvr}(\text{dBm}) = \text{EIRP}_{TX} + \text{FSPL} - 30 \tag{2}$$

where:

d = *distance from transmitter* ~ 19,000 meters (varies depending on orbit and time)

λ = *wavelength* ~ 0.19 meters

EIRP = effective isotropic radiated power ~ 26.50 dBW

$$P_{rcvr}(\text{dBm}) = 26.50 \pm 10 \times \log_{10}\left[\left(\frac{4\pi 19000}{0.19}\right)^2\right] - 30 = -125.48 \text{ dBm} \tag{3}$$

We can supplement this theoretical analysis with experimental data from the US Department of Transportation (DOT) [45]. Through anionic chamber measurements evaluating the threat of interference from cellular LTE towers (at 1530 MHz) on LEO GPS reception, DOT calculated a receiver threshold of -73 dBm for near-band interference on two NASA platforms [45, p. 110]. As our attacker can jam directly in the L1 band, rather than the adjacent LTE frequencies, we can reasonably assume equivalent or greater interference at this threshold.

2) Simulation Process

Our physical simulation consists of two sub-components – an astrodynamics model for CubeSat separation and an RF interference model. In the astrodynamics model, we replicate the separation of a CubeSat from a P-Pod deployer into LEO. This is implemented in FreeFlyer, a commercial space mission planning tool [46]. The CubeSat ejects from the launch vehicle through a contra-velocity maneuver at 2 m/s as is typical for a 4 kg CubeSat [47]. The CubeSat and launch vehicle are propagated

for a two-hour period following separation, and a separation vector is calculated between the two objects at regular one-minute intervals.

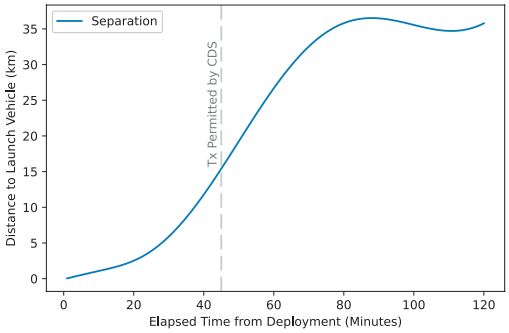
These separation vectors are then leveraged in RF interference simulations. We replicate RF dynamics using MATLAB's Antenna Toolbox, a commercial communications system simulation and development toolkit [48]. Two transmitters are modeled: an L1 GPS transmitter based on the aforementioned P_{rcvr} characteristics and a CubeSat jammer with varying EIRPs from 1–10W. A GPS receiver is replicated on board the rocket. Antenna positions are derived based on the separation vectors calculated in the astrodynamics model and used to compute signal-to-interference-plus-noise ratios (SINR) and $P_{jammer\ at\ rcvr}$(dBm) at regular one-minute intervals.

Under benign conditions ($P_{jammer\ \ at\ \ rcvr}$(dBm) = 0), our model computes: $P_{gps\ at\ rcvr}(dBm)$= -125.48, and $SINR(dB)$= -21.41. These values align with our analysis in Section 5.B.1 and prior work, suggesting reasonable fidelity [43], [49].

C. Results and Evaluation

Figure 2 summarizes the output of our astrodynamics model. Note that the separation vector of magnitude does not increase linearly. This is a result of the relative orbital motion of the CubeSat and LV, both of which are in LEO at time of deployment. In our threat model, the attacker does not adhere to the 45-minute radio silence window mandated by the CDS. This means that it can jam immediately after separation and at close proximity to the LV.

FIGURE 2: CUBESAT SEPARATION FROM LV OVER TIME



Incorporating these results into our interference model shows that the attacker is capable of degrading GPS signal quality (see Figure 3). As expected, the attack is most effective at higher power levels and during the first few minutes following separation.

Using the aforementioned DOT near-band threshold of -73 dBm gives a conservative estimate of 20–40 minutes of disruption depending on amplifier power (see Figure 4).

FIGURE 3: SINR AT LV RECEIVER DURING ATTACK

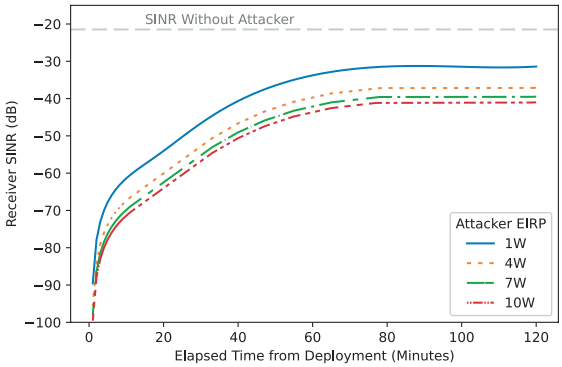
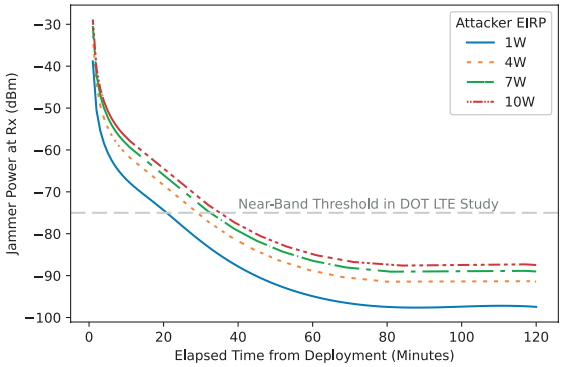


FIGURE 4: JAMMER POWER AT LV RECEIVER DURING ATTACK



To further validate these bounds, we can convert the SINR to Carrier-to-Noise-plus-Interference Density ratio C/N_{O+I}, assuming a typical front-end bandwidth (BW) of 4e6 Hz and applying the conversion method presented in [49] and in Equation 4:

$$C/N_{O+I}(dB\text{–}Hz) = SINR + 10 * \log_{10}(BW) \quad (4)$$

Standard GPS L1 receivers function at C/N_Os between 35 and 55 dB-Hz, with complete loss of signal acquisition below 28 dB-Hz – although this can vary depending on specific hardware conditions [50]. This suggests that our attacker can have a severe impact on GPS quality, keeping C/N_{O+I} below 28 dB-Hz for upwards of 45 minutes at low EIRPs and throughout the simulated period at higher EIRPs (SINR ≤ -38 dB). It

may be prudent to assume that GPS receivers on LVs have access to the wider 20.46 MHz P(Y) frequencies restricted for military use. If this were the case, an attacker would be weaker, but could still expect 30–60 minutes of successful disruption (SINR $\leq$ -45 dB).

In short, these results suggest it is physically plausible for COTS CubeSat hardware to introduce meaningful disruptions to LV GPS reception on the scale of tens of minutes to several hours depending on mission hardware. While operationalizing such an attack would take significant effort, the low cost and accessibility of CubeSat hardware and launch capacity make it well within the means of state-sponsored attackers. Moreover, the reputational risk of attack failure or attribution is limited as key forensic evidence of the attack would be trapped 1,000 km in the sky.

D. Mitigations and Future Work

The scenario considered here is but one of many possible manifestations of our threat model. The underlying vulnerability proposed here has less to do with GPS reception than with the implicit trust dynamics in secondary payload integration. One promising avenue for future work might thus be to build on this adversarial analysis to identify other technical attack vectors of interest (e.g., premature hardware deployment to jam P-Pod deployers).

Our own RFI scenario also leaves room for future work. Due to limited public information, we could not account for the specific AFTS design. AFTS systems may already have a variety of undocumented defenses, such as leveraging multi-constellation GNSS data, elevating the importance of accelerometer readings in the case of GNSS anomalies, or employing various jamming resistance techniques [51]. To the extent that such mitigations are not implemented, they also represent feasible technical steps towards mitigating the attacks proposed here.

At a high level, our research suggests ample opportunity for future work in adjusting trust models around CubeSat integration policies. This is complex, as CubeSats are built under aggressive timeline and budgetary constraints. However, certain properties – such as the validity of hardware interrupts, operational frequencies of RF hardware, or behavior during DITL testing – may be of sufficient importance to merit the added cost of third-party validation. Launch operators may consider offering expedited certification routes for certain pre-approved COTS components, such as antennas which lack capabilities in sensitive frequencies, to reduce compliance costs. Similarly, they may consider allowing developers to gain trust over time, easing the pathways to large-scale CubeSat deployments while still mitigating the risks from naïve or fraudulent first-time developers.

In short, a comprehensive review of the existing integration certification process from an adversarial perspective is beyond the scope of this paper but represents an intuitive next step for launch operators and regulators concerned about potential harm from compromised or malicious third-party payloads.

6. CONCLUSION

In this paper, we have presented the case that strong political and strategic motivations exist for attacks targeting space launch missions. Moreover, we present, to our knowledge, the first cyber-physical threat model targeting LVs through a secondary payload.

While existing CubeSat safety standards employed in the integration and certification process initially appear to constrain cyber adversaries, we find that unverified trust assumptions underpin the real-world practice of this safety qualification process. When considered in the context of a sufficiently motivated malicious cyber adversary, many safety protections appear trivially circumventable.

The implications of this are evaluated experimentally through physical simulations of a novel space-to-space radio interference attack scenario targeting a modern LV. Our results demonstrate that inexpensive CubeSat hardware has sufficient physical capabilities to potentially threaten the reliability of key safety metrics during launch. We further considered how future work might identify related attacks against other launch systems and isolated steps towards mitigating both this specific attack and others of this nature.

For hundreds of satellite operators, transnational launch collaboration has brought space closer than it has ever been. It offers access for start-ups, universities, and states who would otherwise be unable to reach orbit. Moreover, it fosters key links for communication and diplomacy between scientists and engineers in otherwise deeply sensitive domains. However, trust is a keystone component of sustained cooperation. Ensuring security against both cyber and physical risks will be critical to reaping sustained benefits from globalized launch services.

REFERENCES

[1] E. Howell. “Ariane 5 Rocket Lofts 2 Satellites on Milestone 100th Launch.” Space.com. https://www.space.com/41936-ariane-5-rocket-aces-100th-launch.html (accessed Sep. 22, 2020).

[2] E. Howell. “Delta IV Heavy: Powerful Launch Vehicle.” Space.com. https://www.space.com/40360-delta-iv-heavy.html (accessed Sep. 22, 2020).

[3] M. Sheetz. “Elon Musk touts low cost to insure SpaceX rockets as edge over competitors.” CNBC.com. https://www.cnbc.com/2020/04/16/elon-musk-spacex-falcon-9-rocket-over-a-million-dollars-less-to-insure.html (accessed Sep. 22, 2020).
[4] J. Puig-Suari, C. Turner, and W. Ahlgren, “Development of the standard CubeSat deployer and a CubeSat class PicoSatellite,” *2001 IEEE Aerospace Con. Proc. (Cat. No.01TH8542)*, vol. 1, pp. 1/347–1/353, Mar. 2001, doi: 10.1109/AERO.2001.931726.
[5] E. Kulu. “Nanosats Database.” Nanosats Database. [Online]. Available: https://www.nanosats.eu/tables.html (accessed Sep. 24, 2020).
[6] EnduroSat. “1U CubeSat Platform.” EnduroSat.com. https://www.endurosat.com/cubesat-store/all-cubesat-modules/1u-cubesat-platform/ (accessed Sep. 24, 2020).
[7] Nanoracks. “ISS Deployment.” Nanoracks.com. https://nanoracks.com/products/iss-deployment/ (accessed Sep. 24, 2020).
[8] Innovative Solutions in Space. “ISIS ISIPOD 3-Unit CubeSat deployer.” CubeSatShop.com. https://www.cubesatshop.com/product/3-unit-cubesat-deployer/ (accessed Sep. 24, 2020).
[9] CSSWE, *English: The CSSWE CubeSat and PPOD just prior to integration*, 2012. [Online Image]. Available: https://commons.wikimedia.org/wiki/File:CSSWE_CubeSat_and_PPOD_prior_to_integration.png. License: CC-BY-SA-3.0.
[10] C. C. Helms, “A Survey of Launch Services 2016–2020,” in *AIAA Propulsion and Energy 2020 Forum*, AIAA, 2020.
[11] eoPortal. “Vega PoC flight for SSMS.” 2020. https://directory.eoportal.org/web/eoportal/satellite-missions/v-w-x-y-z/vega-ssms (accessed Dec. 2, 2020).
[12] Northrop Grumman. “Minotaur Rocket.” NorthropGrumman.com. https://www.northropgrumman.com/space/minotaur-rocket (accessed Dec. 2, 2020).
[13] W. Graham. “Russia’s Rokot vehicle successfully launches Geo-IK-2 satellite.” NASASpaceFlight.com. https://www.nasaspaceflight.com/2019/08/russias-rokot-geo-ik-2-satellite/ (accessed Dec. 3, 2020).
[14] P. Olbrich and D. Shim, “Symbolic practices of legitimation: exploring domestic motives of North Korea’s space program,” *Int. Relat. Asia Pac*., vol. 19, no. 1, pp. 33–61, Jan. 2019, doi: 10.1093/irap/lcx004.
[15] Defense Intelligence Agency, “Challenges to Security in Space,” 2019. [Online]. Available: https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf
[16] J. Pavur and I. Martinovic, “The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space,” in *2019 11th Int. Conf. on Cyber Conflict (CyCon)*, 2019, vol. 900, pp. 1–18.
[17] J. C. Mauduit, “Collaboration around the International Space Station: science for diplomacy and its implication for US-Russia and China relations,” *Proc. 7th Ann. SAIS Asia Conf. (SAIS 2018)*, Feb. 17, 2017. [Online]. Available: https://swfound.org/media/205798/sais-conference-jcmauduit-paper.pdf
[18] M. Byers, “Cold, dark, and dangerous: international cooperation in the arctic and space,” *Polar Record,* vol. 55, no. 1, pp. 32–47, Jan. 2019, doi: 10.1017/S0032247419000160.
[19] S.-C. Wang, “The Making of New ‘Space’: Cases of Transatlantic Astropolitics,” *Geopolitics*, vol. 14, no. 3, pp. 433–461, Aug. 2009, doi: 10.1080/14650040802693820.
[20] E. L. Chalecki, “Knowledge in Sheep’s Clothing: How Science Informs American Diplomacy,” *Diplomacy & Statecraft*, vol. 19, no. 1, pp. 1–19, Mar. 2008, doi: 10.1080/09592290801913676.
[21] C. Davenport. “Implication of sabotage adds intrigue to SpaceX investigation.” *The Washington Post*. Sep. 30, 2016. https://www.washingtonpost.com/business/economy/implication-of-sabotage-adds-intrigue-to-spacex-investigation/2016/09/30/5bb60514-874c-11e6-a3ef-f35afb41797f_story.html (accessed Dec. 11, 2020).
[22] RT International. “Sabotage considered in Proton rocket crash – investigator.” RT.com. May 29, 2014. https://www.rt.com/news/162228-proton-rocket-failure-sabotage/ (accessed Dec. 11, 2020).
[23] F. Weir, “Russia hints foreign sabotage may be behind space program troubles,” *Christian Science Monitor*, Jan. 10, 2012. https://www.csmonitor.com/World/Global-News/2012/0110/Russia-hints-foreign-sabotage-may-be-behind-space-program-troubles/ (accessed Dec. 11, 2020).
[24] D. Werner. “Small satellite sector grapples with cybersecurity requirements, cost.” SpaceNews.com. August 8, 2018. https://spacenews.com/small-satellite-sector-grapples-with-cybersecurity-requirements-cost/ (accessed Sep. 21, 2020).
[25] K. W. Ingols and R. W. Skowyra, “Guidelines for Secure Small Satellite Design and Implementation: FY18 Cyber Security Line-Supported Program,” MIT Lincoln Laboratory Lexington United States, Feb. 2019. Accessed: Sep. 24, 2020. [Online]. Available: https://apps.dtic.mil/sti/citations/AD1099003
[26] M. Langer and J. Bouwmeester, “Reliability of CubeSats – Statistical Data, Developers’ Beliefs and the Way Forward,” *Proc. 30th Ann. AIAA/USU Conf. Small Satell.,* 2016, [Online]. Available: https://repository.tudelft.nl/islandora/object/uuid%3A4c6668ff-c994-467f-a6de-6518f209962e

[27] M. Swartwout, "You say 'Picosat', I say 'CubeSat': Developing a better taxonomy for secondary spacecraft," in *2018 IEEE Aerosp. Conf.*, pp. 1–17, Mar. 2018, doi: 10.1109/AERO.2018.8396755.
[28] NASA, *CubeSat 101: Basic Concepts and Processes for First-Time CubeSat Developers*. 2017. [Online] Available: https://www.nasa.gov/sites/default/files/atoms/files/nasa_csli_cubesat_101_508.pdf
[29] Cal Poly SLO, *CubeSat Design Specification (CDS) REV 13*, 2014. [Online]. Available: https://blogs.esa.int/philab/files/2019/11/RD-02_CubeSat_Design_Specification_Rev._13_The.pdf
[30] HQ AFSPC/SEK, *Air Force Space Command Manual 91-710, Volume 3*, May 2019. [Online]. Available: https://static.e-publishing.af.mil/production/1/afspc/publication/afspcman91-710v3/afspcman91-710v3.pdf
[31] C. Gebara and D. Spencer, "Verification and Validation Methods for the Prox-1 Mission," *Small Satell. Conf.*, Aug. 2016, [Online]. Available: https://digitalcommons.usu.edu/smallsat/2016/TS8StudentComp/3
[32] Jerry Buxton, *AMSAT Fox-1 DITL Test*. Jan 1, 2015 [Video Recording]. Available: https://www.youtube.com/watch?v=TjGAYvMyz4Q (accessed Dec. 31, 2020).
[33] Department of Defense, "MIL-STD-882E," May 2012. [Online]. Available: https://www.dau.edu/cop/armyesoh/DAU%20Sponsored%20Documents/MIL-STD-882E.pdf
[34] G. L. Prater, "NPSAT1 Missile System Pre-launch Safety Package (MSPSP)," Jun. 2004. Accessed: Jan. 1, 2021. [Online]. Available: https://apps.dtic.mil/sti/citations/ADA424941
[35] SpaceX, "Falcon User's Guide," Apr. 2020. [Online]. Available: https://www.spacex.com/media/falcon_users_guide_042020.pdf
[36] United Launch Alliance, *Delta IV Launch Services User's Guide*, Jun. 2013. [Online]. Available: https://www.ulalaunch.com/docs/default-source/rockets/delta-iv-user's-guide.pdf
[37] L. Valencia, "Autonomous Flight Termination System (AFTS)," 2019, [Online]. Available: https://www.gps.gov/cgsic/meetings/2019/valencia.pdf
[38] FCC. "Space Exploration Technologies Corp. (SpaceX) Experimental License FCC Filings." 2020. https://fcc.report/ELS/Space-Exploration-Technologies-Corp-SpaceX (accessed Jan. 2, 2021).
[39] Space Micro, "µSDR-C Software Defined Radio," 2019. [Online]. Available: spacemicro.com/products/communication-systems/µSDR-CTM%20SOFTWARE%20DEFINED%20RADIO.pdf
[40] Flexitech Aerospace. "Satellite Communication Systems Products." FlexitechAerospace.com. https://flexitechaerospace.com/products/ (accessed Jan. 2, 2021).
[41] CubeSatShop. "Helios deployable antenna." CubeSatShop.com. https://www.cubesatshop.com/product/helios-deployable-antenna/ (accessed Jan. 2, 2021).
[42] I. F. Akyildiz, J. M. Jornet, and S. Nie, "A new CubeSat design with reconfigurable multi-band radios for dynamic spectrum satellite communication networks," *Ad Hoc Nets*., vol. 86, pp. 166–178, Apr. 2019, doi: 10.1016/j.adhoc.2018.12.004.
[43] E. Shehaj, V. Capuano, C. Botteron, P. Blunt, and P.-A. Farine, "GPS Based Navigation Performance Analysis within and beyond the Space Service Volume for Different Transmitters' Antenna Patterns," *Aerospace*, vol. 4, no. 3, Art. no. 3, Sep. 2017, doi: 10.3390/aerospace4030044.
[44] FCC, "GPS L1 Link Budget." [Online]. Available: https://apps.fcc.gov/els/GetAtt.html?id=110032&x=
[45] US Department of Transportation, "Global Positioning System (GPS) Adjacent Band Compatibility Assessment," 2017. [Online]. Available: https://www.transportation.gov/sites/dot.gov/files/docs/subdoc/186/dot-gps-adjacent-band-final-report.pdf
[46] ai-solutions, *FreeFlyer® Software*, v7.6 (Mission) [Commercial Software]. 2018. Available: https://ai-solutions.com/freeflyer-astrodynamic-software/
[47] W. Lan, R. Munakata, R. Nugent, and D. Pignatelli, "Poly Picosatellite Orbital Deployer Mk. III Rev. E User Guide," 2014. [Online]. Available: https://static1.squarespace.com/static/5418c831e4b0fa4ecac1bacd/t/5806854d6b8f5b8eb57b83bd/1476822350599/P-POD_MkIIIRevE_UserGuide_CP-PPODUG-1.0-1_Rev1.pdf
[48] MathWorks, *MATLAB Antenna Toolbox*, v2020b [Commercial Software]. 2020. Available: https://uk.mathworks.com/products/antenna.html
[49] Inside GNSS, "Measuring GNSS Signal Strength," *Inside GNSS - Global Navigation Satellite Systems Engineering, Policy, and Design*, Dec. 2, 2010. [Online]. Available: https://insidegnss.com/measuring-gnss-signal-strength/
[50] A. Brierley-Green, "Global Navigation Satellite System Fundamentals and Recent Advances in Receiver Design," presented at IEEE Long Island Section, Sep. 2017, [Online]. Available: https://www.ieee.li/pdf/viewgraphs/gnss_fundamentals.pdf
[51] G. X. Gao, M. Sgammini, M. Lu, and N. Kubo, "Protecting GNSS Receivers From Jamming and Interference," *Proc. IEEE*, vol. 104, no. 6, pp. 1327–1338, Jun. 2016, doi: 10.1109/JPROC.2016.2525938.