2019 11th International Conference on Cyber Conflict:
Silent Battle
T. Minárik, S. Alatalu, S. Biondi,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2019 © NATO CCD COE Publications, Tallinn

The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space

James Pavur
DPhil Researcher
Cybersecurity Centre for Doctoral Training
Oxford University
Oxford, United Kingdom
james.pavur@cybersecurity.ox.ac.uk

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

Abstract: Satellites have revolutionized military strategy and the dynamics of national power. However, satellites themselves are fragile and can be destroyed by even miniscule projectiles. Anti-Satellite Weapons (ASATs) which exploit this weakness have long been prophesied as the Achilles heel of space power; yet orbit has remained relatively peaceful for more than sixty years.

As the threat of cyber attacks against space assets looms, the impact that cyberspace will have on stability in outer space is not well understood. This paper presents a strategic analysis of the impact of cyber weapons on three key stabilizing factors which have thus far contributed to peace in space. Based on this analysis, it contends that cyber-ASATs threaten the foundations of space's longstanding stability due to their high accessibility, low attributability, and low risk of collateral damage.

This conjecture is tested experimentally though the development of a simulated cyber-ASAT capability targeting one small component of satellite operations: space situational awareness data. By leveraging orbital simulations and genetic algorithms, we demonstrate the ability to artificially alter debris collision forecasts and cause direct harm to critical space systems without firing a single rocket. The attack method is tested in realistic simulations and shown to have a high success rate against real-world satellites of vital strategic importance.

Our interdisciplinary approach unifies strategic analysis with technical experimentation to present the case that cyber-ASATs are not merely a distant theoretical threat, but a real and present danger to the balance of power in space.

Keywords: *satellites, ssa, cyber-ASAT, space, space power, ASAT*

1. INTRODUCTION

In 1958, then US Senator Lyndon Johnson predicted that ‘control of space means control of the world’ [1, p. 287]. 33 years later, Operation Desert Storm, widely referred to as ‘the first space war’, validated this prophecy [2]. Overwhelming US dominance during the 100-hour ground war was directly attributable to the support of over 60 positioning, communications and reconnaissance satellites [3]–[5].

Modern space power has created a world in which ‘no enemy can withstand a frontal assault upon U.S. forces due to the American ability to sense, move, and strike with precision’ [6, p. 236]. As the world becomes increasingly multipolar, many other states are expected to seek the same prestige and military power, associated with membership of the ‘space club’ [7], [8]. Over the past half-century, space has become the ‘ultimate high ground’ for information age warfare [9], [10, p. 714].

This strategic vitality stands at odds with critical vulnerability. Satellites are lightweight and fragile devices moving at incredible speeds. A marble-sized projectile or debris particle in orbit could strike a satellite with the force of a one-ton object falling from a height of five storeys [11]. In the seminal days of space strategy, this physical weakness was thought to undermine the strategic utility of space itself [12, Ch. 5]. The rise of anti-satellite weapons (ASATs), which exploit this weakness, has long been prophesied to bring about the end of space power. However, somehow, orbit has remained remarkably peaceful.

As space systems become increasingly interconnected and computationally complex, new concerns about the threat of cyber-attacks have been raised [13]. However, the strategic implications and technical feasibility of cyber-ASATs are not well understood. This paper seeks to unite strategic and technical perspectives on cyber attacks in space as a starting point for policymakers and technicians to address these threats.

2. CONTRIBUTIONS

The core motivator for our research was to credibly assess if cyber-ASAT capabilities pose a fundamental challenge to the dynamics of orbital peace, or if the structural factors which have stabilized space for the past half-century will continue to endure.

To this end, this paper begins with a brief overview of three widely recognized stabilizing forces: limited accessibility, attributable norms and environmental interdependence. We then contribute what we believe to be the first high-level strategic consideration of cyber-ASATs with regard to each of these factors. We predict that cyber-ASATs can undermine all three, due to their widespread accessibility, weak norms and attribution, and environmental indifference.

To bolster these theoretical claims, this paper adopts an interdisciplinary approach, leveraging an experimental case study to verify the technical feasibility of the cyber-ASATs that it predicts will emerge. This case study revolves around the creation and simulation of a cyber-ASAT capability, targeting space situational awareness (SSA) data. Our attack method combines orbital simulations and genetic algorithms to artificially alter debris collision projections and induce harmful satellite manoeuvres. The attack is verified through experimental simulations against more than 100 major communications satellites; we demonstrate a greater than 90% success rate against all targets.

Together, our experimental findings and strategic assessment suggest that cyber-ASATs are not merely another tool in the anti-satellite arsenal, but a real and present danger to the very foundations of stability in orbit.

3. STABILITY IN SPACE

Given the uncomfortable combination of high dependency and low survivability, one might expect to observe frequent attacks against critical military assets in orbit. However, despite decades of recurring prophesies of impending space war, no such conflict has broken out [14]–[18]. It is true that a handful of space security crises have occurred; most notably, the 2007 Chinese anti-satellite weapon (ASAT) test and the 2008 US ASAT demonstration in response [19]. Moreover, a recent Centre for Strategic and International Studies report suggests increasing interest in attacking US space assets, particularly among the Chinese, Russian, North Korean and Iranian militaries [20]. Overall, however, the space domain has remained puzzlingly peaceful. In this section, we outline three major contributors to this enduring stability: limited accessibility, attributable norms, and environmental interdependence.

A. Limited Accessibility

Space is difficult. Over 60 years have passed since the first Sputnik launch and only nine countries (ten including the EU) have orbital launch capabilities. Moreover, a launch programme alone does not guarantee the resources and precision required to operate a meaningful ASAT capability. Given this, one possible reason why space wars have not broken out is simply because only the US has ever had the ability to fight one [21, p. 402], [22, pp. 419–420].

Although launch technology may become cheaper and easier, it is unclear to what extent these advances will be distributed among presently non-spacefaring nations. Limited access to orbit necessarily reduces the scenarios which could plausibly escalate to ASAT usage. Only major conflicts between the handful of states with ‘space club’ membership could be considered possible flashpoints. Even then, the fragility of an attacker’s own space assets creates de-escalatory pressures due to the deterrent effect of retaliation. Since the earliest days of the space race, dominant powers have recognized this dynamic and demonstrated an inclination towards de-escalatory space strategies [23].

B. Attributable Norms

There also exists a long-standing normative framework favouring the peaceful use of space. The effectiveness of this regime, centred around the Outer Space Treaty (OST), is highly contentious and many have pointed out its serious legal and political shortcomings [24]–[26]. Nevertheless, this *status quo* framework has somehow supported over six decades of relative peace in orbit.

Over these six decades, norms have become deeply ingrained into the way states describe and perceive space weaponization. This *de facto* codification was dramatically demonstrated in 2005 when the US found itself on the short end of a 160-1 UN vote after opposing a non-binding resolution on space weaponization. Although states have occasionally pushed the boundaries of these norms, this has typically occurred through incremental legal re-interpretation rather than outright opposition [27]. Even the most notable incidents, such as the 2007-2008 US and Chinese ASAT demonstrations, were couched in rhetoric from both the norm violators and defenders, depicting space as a peaceful global commons [27, p. 56]. Altogether, this suggests that states perceive real costs to breaking this normative tradition and may even moderate their behaviours accordingly.

One further factor supporting this norms regime is the high degree of attributability surrounding ASAT weapons. For kinetic ASAT technology, plausible deniability and stealth are essentially impossible. The literally explosive act of launching a rocket cannot evade detection and, if used offensively, retaliation. This imposes high diplomatic costs on ASAT usage and testing, particularly during peacetime.

C. Environmental Interdependence

A third stabilizing force relates to the orbital debris consequences of ASATs. China's 2007 ASAT demonstration was the largest debris-generating event in history, as the targeted satellite dissipated into thousands of dangerous debris particles [28, p. 4]. Since debris particles are indiscriminate and unpredictable, they often threaten the attacker's own space assets [22, p. 420]. This is compounded by Kessler syndrome, a phenomenon whereby orbital debris 'breeds' as large pieces of debris collide and disintegrate. As space debris remains in orbit for hundreds of years, the cascade effect of an ASAT attack can constrain the attacker's long-term use of space [29, pp. 295–296]. Any state with kinetic ASAT capabilities will likely also operate satellites of its own, and they are necessarily exposed to this collateral damage threat. Space debris thus acts as a strong strategic deterrent to ASAT usage.

4. THE APPEAL OF THE CYBER-ASAT

The overall effect of cyber-attacks vis-à-vis this strategic stability in space is not well understood. The general need to incorporate cyber risk into satellite mission planning and various legal parallels between the cyber and space commons have attracted some attention [13], [30]. However, cyber weapons in space are often thought of as just one tool among many in the growing ASAT arsenal [31], [32]. In this section, we argue that cyber weapons pose unique strategic threats by undermining the stabilizing dynamics of the *status quo*. Specifically, we contend that cyber-ASATs are accessible, difficult to deter, and environmentally indifferent.

A. Widespread Accessibility

Cyber-attack capabilities are far more widespread than orbital launch technology. In 2017, a former deputy director of the National Security Agency estimated that 'well over 100' countries could harm the US with offensive cyber capabilities [33]. This is over ten times the number of independent spacefaring nations and 50 times the number with proven ASAT technology. Of course, mere possession of cyber capabilities does not guarantee that these can be used against satellites. Nevertheless, this suggests that, for many actors, digital attacks are far more feasible than the creation of national space weapons programmes.

This calculus is further bolstered by the fact that cyber attack capacities which could threaten satellites may apply to other unrelated systems. Thus, even if space is not the primary motivator for cyber-weapons development, one can expect states to cultivate offensive cyber capabilities which can be repurposed for ASAT attacks [34]. Moreover, while the idea of terrorist cells developing orbital spaceflight programmes appears almost comically absurd, even non-state actors have demonstrated sophisticated cyber capabilities [20], [35].

B. Detterence Challenges

International norms influencing cyber combat are both younger and weaker than their space parallels. Scepticism has emerged as to the possibility of ever developing meaningful normative backstops against cyber attacks [36]. Nevertheless, much of the cyber policy community remains optimistic about the eventual cultivation of global norms – a debate which is well beyond the scope of this paper. At present, however, the cyber norms regime has an indisputably worse track record than even the oft-maligned OST.

Moreover, unlike kinetic ASATs, cyber attacks have low risk of attribution and, by extension, low risk of retaliation (and its associated deterrent effect). There has been a great deal of recent debate over the ultimate attributability and deterrability of sophisticated cyber operations [37]–[39]. However, few on either side would contend that cyber attacks are as attributable as the launch of an orbital rocket from sovereign territory. A kinetic ASAT would be noticed and credibly attributed within minutes, but the average data breach evades detection for 200 days, even for critical systems [40]. A cyber-ASAT could lie dormant on target systems for years before triggering at a critical moment. Moreover, this stealth and deniability provides cover for states which publicly encourage the peaceful use of space while they covertly develop ASAT capabilities.

C. Environmental Indifference

Finally, cyber-ASATs undermine the ecological dynamics constraining space weaponization. Actors with cyber-ASAT capabilities may have significantly less strategic dependence on the space environment than the major spacefaring powers. As such, the deterrent effect of collateral damage through space debris would be reduced. Although debris in space can have negative commercial effects on almost all countries, in times of war, this may be an acceptable cost for smaller nations with asymmetric weaknesses. Cyber-ASATs also raise the new spectre of non-destructive ASATs. For example, an exploit which disables or reduces the lifetime of a targeted satellite (e.g. by wasting fuel) could prove environmentally palatable even to states with exposure to space debris.

D. Feasibility of a Cyber-ASAT

In short, cyber-ASATs appear to threaten the foundations of a half-century's stability in orbit. However, premature predictions of instability have become a long-standing tradition in the space policy world. Nearly every major advancement in space technology has been incorrectly heralded as the harbinger of space power's demise. Flawed assumptions about underlying technologies can easily snowball into hyperbolic political strategic theory.

To hold our claims to a higher standard, we have devised a practical case study on the development and use of a cyber-ASAT. In it, we target one aspect of space-flight operations: the collection and use of space situational awareness (SSA). We design and simulate a cyber-attack method that has all three attributes suggested by our strategic analysis. Specifically, our attack uses widely available technology, is stealthy, and minimizes collateral damage. This allows us not only to present the *theoretical* dangers of cyber-ASATs; but to assess their *practical* threat to the *status quo*.

5. SSA: TERRESTRIAL TARGET, CELESTIAL EFFECTS

A. Role of SSA Data

At present, more than 21,000 pieces of orbital debris measuring larger than 10cm in diameter are tracked by the US government [41]. Well over 100 million additional smaller objects are believed to exist but are too small to track reliably. These objects whizz overhead at velocities in excess of 8 km/s and collide at speeds exceeding 10 km/s, meaning that collisions with even miniscule objects can cause catastrophic satellite failures [41].

To safely navigate this ever-growing debris field, operators depend on reliable tracking of orbital hazards. This data is a core component of SSA, which is used by orbital simulation models to predict collisions and inform day-to-day flight control decisions.

Even with modern SSA technologies, collisions still take place. For example, in March 2013, a piece of debris from the 2007 Chinese ASAT test collided with a Russian nanosatellite [42]. Without accurate and reliable SSA data, such incidents would occur far more frequently. In 2017 alone, more than 300,000 potential collision events were identified in US government SSA, 655 of which crossed 'emergency' proximity thresholds for pass distances [43].

B. SSA Data Sources

Although mathematical modelling makes it possible to roughly project orbital motion, complex gravitational and environmental interactions quickly degrade estimates. Reliable SSA data therefore requires frequent observational measurements. The primary sensors employed are radar platforms used in missile defence [44]. This data is supplemented with optical telescopes, ground-based lasers and some space-based observation platforms [44], [45].

The principal constraint on SSA capabilities is often geographic rather than technological. SSA sensors cannot detect objects which do not cross their visible horizon. Large networks of sensors distributed across the planet are thus needed to maintain a complete SSA data repository. This geographic distribution requirement has caused heavy centralization of SSA data into a handful of large repositories.

The Space Surveillance Network (SSN), operated by the US military, is the most widely used and accurate repository. It is believed that only the SSN has global coverage for small objects (~10 cm) [45]. The next closest competitor is the Russian Space Surveillance System, which operates in many former Soviet states and has decent coverage over the northern hemisphere and for larger objects [46]. The Chinese government also operates a network, largely constrained by China's borders [46]. Other networks include the European Space Surveillance System and smaller systems operated by Japan, India, Korea, Canada, Kazakhstan, and Ukraine [44], [46]. Alone, these are unlikely to provide adequate SSA. Commercial SSA products have also begun to emerge, although none offer complete catalogues for objects even 20cm in diameter [45].

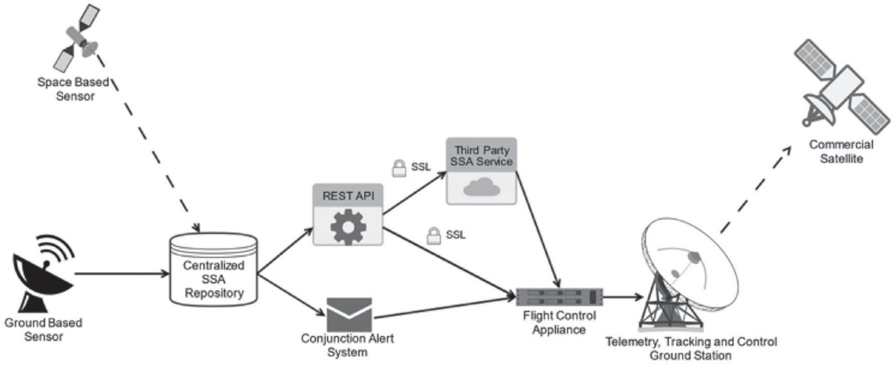
The US freely shares its SSA data through the Space-Track.org platform [47], [48]. Typically, a satellite operator will download SSA from Space-Track and use it to perform conjunction analysis for space missions. Space-Track provides opt-in conjunction alerts and collision avoidance services, but many operators still perform these tasks in-house [47]. Beyond Space-Track, Russia operates a similar scheme through the semi-governmental International Scientific Optical Network (ISON), but usage is far less common [45].

Game-theoretic studies of SSA have demonstrated that these sharing schemes benefit all stakeholders [49]. Intuitively, this makes sense, as the US gains little by concealing SSA data from Russian military operators and causing a collision which would threaten both countries. As a result, a trans-national trust dynamic has emerged around SSA.

C. Value of SSA as Cyber Target

Given that most actors lack the capability to independently verify SSA claims, this trust dynamic is essentially blind. As repositories are highly centralized and hard to verify, a small change to the integrity of the central repository could have massive effects.

FIGURE 1: A NOTIONAL OVERVIEW OF THE SSA DATA FLOW AND POTENTIAL TARGETS.



A cyber attacker might gain access to such repositories through Stuxnet-esque attacks against sensors, direct compromise of centralized databases, modification of data stored at the flight controller's operation centre, exploitation of third-party SSA aggregation services, or alteration of data in transit (Figure 1). Some components of this infrastructure (such as radar sensors or encrypted connections) might require high degrees of sophistication to attack; while others (such as SSA-sharing APIs) may be within the means of most cyber adversaries.

Using this access, an attacker may alter data to effect satellite operator behaviour. For example, an attacker might manipulate an SSA repository to make a near-miss between a debris object and a targeted satellite appear as a collision. This would cause the victim to undertake collision avoidance manoeuvres, shortening the satellite's lifetime through fuel wastage. The reverse attack could also be executed, where an attacker conceals a projected collision and destroys the targeted satellite, all without launching a single rocket.

In essence, SSA exploitation elevates simple integrity compromises into Cyber-ASAT capabilities. Furthermore, the fuel wastage attack scenario does not threaten collateral debris damage. As such, an attack against SSA data meets all three design objectives outlined in section 3.

6. CASE STUDY: SIMULATING ATTACKS AGAINST SSA

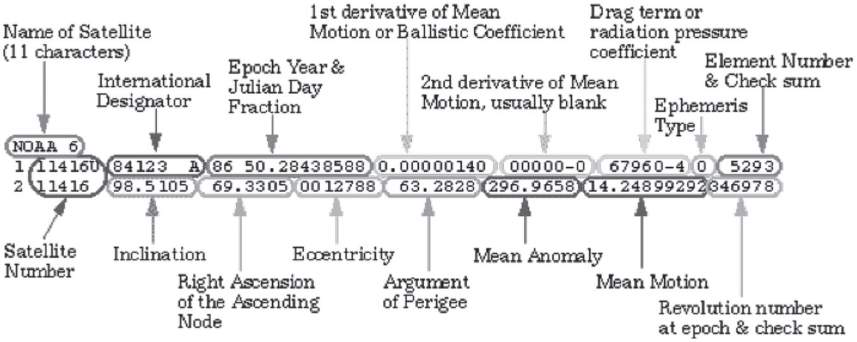
A. Experimental Design and Assumptions

We elected to assess the technical feasibility of attacks on SSA repositories through simulations with a commercial spaceflight planning tool [50].

The simulated attacker's overall objective was to cause an arbitrary satellite in Low Earth Orbit to take unnecessary collision-avoidance manoeuvres over the next 72 hours (the current SSN emergency notification threshold). We assumed that our attacker wished to be stealthy and that significant modification of SSA data (such as the creation of new debris objects) would be detected. Finally, we granted that the attacker had already obtained the ability to modify data through traditional cyber exploitation techniques (e.g. malware installed on the SSA web servers).

Target data was assumed to be in the widely used two-line element (TLE) format (Figure 2). This format is used to distribute projections from Space-Track.org. The format was originally designed to fit on two 80-column punch cards; no security features or significant revisions have been made since its adoption by NORAD in the 1970s [51].

FIGURE 2: THE TLE EPEHEMERIS DATA FORMAT [52]. STARRED PARAMETERS ARE TARGETED BY OUR ATTACK.


Name of Satellite (11 characters)
1st derivative of Mean Motion or Ballistic Coefficient
Drag term or radiation pressure coefficient
Element Number & Check sum
International Designator
Epoch Year & Julian Day Fraction
2nd derivative of Mean Motion, usually blank
Ephemeris Type
NOAA 6
1 11416U 84123 A 86 50.28438588 0.00000140 00000-0 67960-4 0 5293
2 11416 98.5105 69.3305 0012788 63.2828 296.9658 14.24899292346978
Satellite Number
Inclination
Right Ascension of the Ascending Node
Eccentricity
Argument of Perigee
Mean Anomaly
Mean Motion
Revolution number at epoch & check sum

The simulations themselves were built using real-world data from the US SSN. Projections were propagated with the SGP4 propagator provided by Air Force Space Command and recommended for usage with TLE data [53].

B. Attack Method

Our proposed attack consists of three stages: acquisition, perturbation, and generation. In the acquisition phase, five 'near-miss' debris objects are selected as candidates for potential tampering. In the perturbation phase, the SSA data describing these objects are strategically altered to artificially cause a collision projection. Finally, in the generation stage, these alterations are merged with authentic data to create a falsified TLE entry for insertion into the SSA repository.

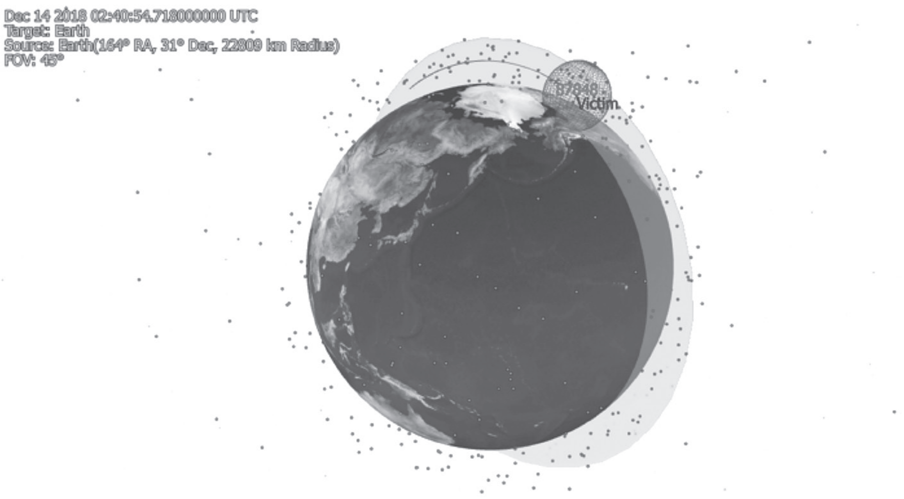
a) Acquisition stage

To begin, an attacker must provide accurate TLEs characterizing a victim satellite's orbit and any debris objects to be considered. This information is readily available online.

Our attack tool automatically synchronizes these TLEs to a common starting epoch. From this epoch, the debris objects and victim satellite are propagated to project their locations over a simulated 72-hour period, subdivided into 10-second intervals.

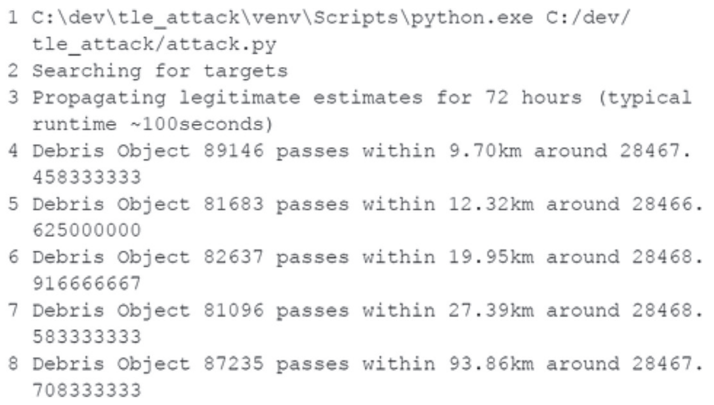
At each interval, a three-step filter is employed to remove irrelevant debris objects (Figure 3). First, we select only debris objects currently inside the victim satellite's orbit plane (represented by a 100km deep cylinder, centred at the Earth's core and oriented along the victim's orbit). Second, we remove debris with altitudes outside a range bounded by the victim satellite's perigee (lowest orbital altitude) and apogee (highest orbital altitude). Third, we remove debris objects more than 1000km away from the victim satellite in any direction.

FIGURE 3: THE THREE-STEP DEBRIS FILTER. DEBRIS OBJECT 87848 HAS JUST ENTERED A 1000KM SPHERE CENTERED ON THE VICTIM SATELLITE.


Dec 14 2018 02:40:54.718000000 UTC
Target: Earth
Source: Earth(164° RA, 31° Dec, 22809 km Radius)
FOV: 45°
87848
Victim

For any debris which survive this filtering, we calculate the time and distance of closest approach to the victim over a full orbital period. Ultimately, the five objects which pass closest over the whole 72-hour window are selected (as in Figure 4). TLE data for these objects is passed on to the perturbation stage along with times of their closest approaches.

FIGURE 4: TYPICAL ACQUISITION STAGE OUTPUT.



```
C:\dev\tle_attack\venv\Scripts\python.exe C:/dev/
tle_attack/attack.py
Searching for targets
Propagating legitimate estimates for 72 hours (typical
runtime ~100seconds)
Debris Object 89146 passes within 9.70km around 28467.
458333333
Debris Object 81683 passes within 12.32km around 28466.
625000000
Debris Object 82637 passes within 19.95km around 28468.
916666667
Debris Object 81096 passes within 27.39km around 28468.
583333333
Debris Object 87235 passes within 93.86km around 28467.
708333333
```

b) Perturbation Stage

In the perturbation stage, TLEs of the five selected debris objects are altered with the goal of reducing the projected nearest pass distance to the target to less than 1km. This is based on Air Force Space Command guidance that TLEs can be considered accurate to approximately 1km of precision. Any object which passes within this range could thus trigger an anticipated conjunction.

In order to reduce the risk of detection, two further constraints are imposed. First, only four TLE fields (along with the TLE checksum) are subject to modification. Moreover, these fields are altered within certain boundaries (detailed in Table 1). To our knowledge, no study has investigated to what extent, if any, satellite operators vet SSA data for anomalies. As such, these boundaries were selected arbitrarily based on the overall precision of the TLE format (also detailed in Table 1). Decreasing these bounds lowers the chance of detection but increases computational complexity.

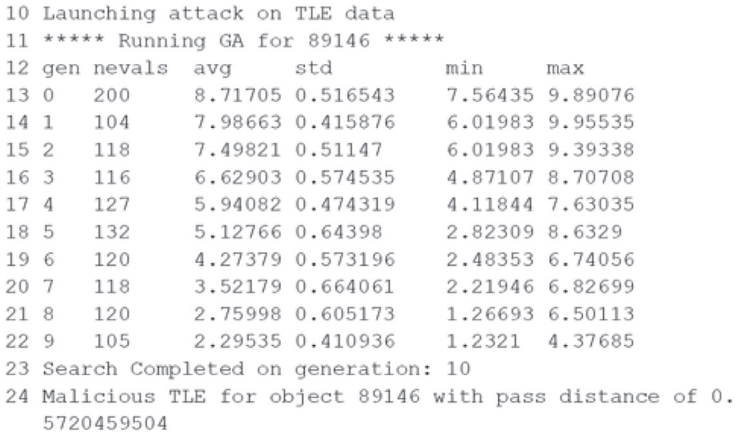
TABLE 1: MODIFIED TLE FIELDS AND BOUNDARIES

TLE Field	Maximum Alteration	TLE Precision
Orbital Inclination	± .1 degrees	.0001 degrees
Right Ascension of the Ascending Node	± .1 degrees	.0001 degrees
Eccentricity	± .01	.0000001
Argument of Perigee	± .1 degrees	.0001 degrees

SGP4, like most orbital projection models, is complex; the overall effect of any given modification over a 72-hour window is non-trivial. However, we can greatly reduce this complexity by recognizing that there is no need to find the *optimal* perturbation set, but rather only an *adequate* set to cause a collision.

This realization allows us to employ a rudimentary genetic algorithm, where we treat the TLE fields themselves as genetic features. Our model's fitness is simply the minimization of nearest pass distance; our initial population size is arbitrarily set to 200 individuals. Over a span of up to 40 generations, each individual is used to generate a fake TLE and propagated for the 3-hour period surrounding the debris object's closest approach (Figure 5). Once a sub-1km pass is found, this result is passed along to the generation stage.

FIGURE 5: TYPICAL PERTURBATION STAGE OUTPUT. IN THIS CASE, A SET OF MODIFICATIONS WAS DETECTED THAT CAUSED DEBRIS OBJECT 89146 TO PASS WITHIN 600M OF THE VICTIM SATELLITE.



```
Launching attack on TLE data
***** Running GA for 89146 *****
gen nevals  avg     std         min     max
0   200     8.71705 0.516543    7.56435 9.89076
1   104     7.98663 0.415876    6.01983 9.95535
2   118     7.49821 0.51147     6.01983 9.39338
3   116     6.62903 0.574535    4.87107 8.70708
4   127     5.94082 0.474319    4.11844 7.63035
5   132     5.12766 0.64398     2.82309 8.6329
6   120     4.27379 0.573196    2.48353 6.74056
7   118     3.52179 0.664061    2.21946 6.82699
8   120     2.75998 0.605173    1.26693 6.50113
9   105     2.29535 0.410936    1.2321  4.37685
Search Completed on generation: 10
Malicious TLE for object 89146 with pass distance of 0.
5720459504
```

Our naïve genetic algorithm may be further optimized. It is likely that a generalized approach, which does not rely on genetic algorithms at all, may be found. However, the operational benefit of finding a pass within 10m versus a pass within 900m is minimal, since both fall within the collision detection radius. Further, given that an attacker has hours, if not days, to calculate these modifications, computational efficiency is far from vital.

c) Generation Stage

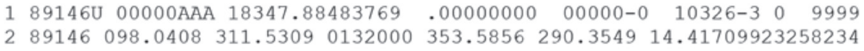
In the generation stage, the results of the five genetic algorithm runs may be compared using two further metrics:

- The proximity of the projected pass caused by a malicious TLE
- The overall magnitude of modifications introduced into a malicious TLE.

The first metric is useful for an attacker who wishes to have the highest likelihood of causing a satellite manoeuvre. The second metric would be more desirable for attackers seeking to minimize the risk of detection. An attacker can also ignore these metrics and simply select the first valid attack found to minimize search time.

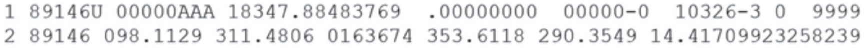
Once a malicious TLE parameter set has been found, its modifications are merged with data from the original debris TLE (as in Figure 6). The result of this process is a new TLE which can be inserted into the SSA database by an attacker as required, completing the attack (Figure 7).

FIGURE 6: A TYPICAL ORIGINAL TLE.



```
1 89146U 00000AAA 18347.88483769  .00000000  00000-0  10326-3 0  9999
2 89146 098.0408 311.5309 0132000 353.5856 290.3549 14.41709923258234
```

FIGURE 7: A TYPICAL MALICIOUS TLE.



```
1 89146U 00000AAA 18347.88483769  .00000000  00000-0  10326-3 0  9999
2 89146 098.1129 311.4806 0163674 353.6118 290.3549 14.41709923258239
```

C. Attack Simulation

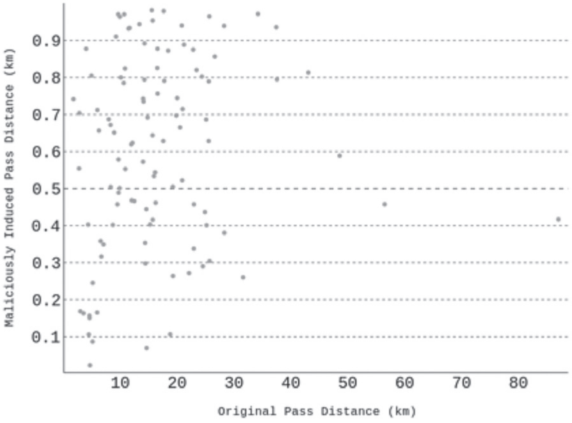
To test this approach experimentally, we simulated attacks against each of 111 satellites in the Iridium constellation. Iridium is a commercial communications service with over one million satellite customers [54]. The network's largest customer is the US Defense Information Systems Agency [55]. For our debris field, we selected 529 objects from Space-Track.org's 'Well-Tracked Analyst Objects of Unknown Origin' dataset [48]. Prior to launching our attack, none of the Iridium satellites were projected to pass within 1km of these objects over a 72-hour window.

In order to simulate attacks against many satellites quickly, we enforced no optimizations in the 'generation' phase. This means that our experiment represents the worst case scenario for our method in terms of pass distance and stealth.

Our technique successfully generated collision events for more than 93% of the Iridium constellation. On average, it took about 12 genetic generations to find a valid attack; the total attack runtime for each object averaged a little over 6 minutes on consumer grade hardware.

Although we accepted any pass under 1km, the mean pass distance of our attack parameters was around 600m and the minimum only 2m. No obvious correlation between original pass distance and malicious pass distance was observed (Figure 8). This suggests that more restrictive boundaries and more demanding proximity requirements are obtainable using this general approach.

FIGURE 8: ORIGINAL AND MALICIOUS PASS DISTANCES FROM THE IRIDIUM ATTACK SIMULATION.



Our findings demonstrate that, once an attacker has compromised the integrity of an SSA repository, elevating this to ASAT capability is quite feasible. With consumer grade hardware and a minimally optimized attack method, we falsified collision projections for over 100 real-world satellites used by the world's largest militaries.

7. CONCLUSION

In this paper, we have argued that the free pursuit of space power has been facilitated by structural features of the space domain. Specifically, we isolated three key features: limited accessibility, attributable norms, and environmental interdependence. We theorized that cyber-attacks can undermine all three of these dynamics and thus pose a structural threat to the long-standing peace in orbit.

To assess these theoretical claims, we designed a cyber-ASAT capability, targeting space situational awareness. Our cyber-ASAT was built using widely accessible technologies and minimized both the risk of attribution and collateral damage. This cyber-ASAT was tested in orbital spaceflight simulations and successfully attacked 93% of the strategically vital Iridium satellite constellation, all without firing a single rocket.

Our experimental findings suggest that the rise of cyber-ASATs is not merely a distant technological spectre, but rather a real and present danger. Satellite operators and the states who rely upon them must assess the risks of 'blind trust' information-sharing relationships and, more broadly, the overall cyber-security profile of these systems.

This paper considers only one demonstrative example among many plausible mechanisms for cyber-ASAT capabilities. Future work considering vectors such as on-board malware, compromise of satellite control telemetry, sensor injection, and signal hijacking may help to further characterize this emerging domain. Additionally, there is a clear need for research into defensive mechanisms which prevent such attacks. For example, a statistical approach to anomaly detection in SSA datasets may prove useful in this case. Such research to defend satellites from Cyber-ASATs will be a vital prerequisite for the continued exercise of space power.

Acknowledgments

We extend thanks to a.i. solutions, Inc. for providing research access to the FreeFlyer astrodynamics software used in our spaceflight simulations. J. P. also thanks the Rhodes Trust for funding in support of this research; and the Satellite Applications Catapult, for providing background information on spaceflight operations.

REFERENCES

[1] A. Wilson, *The Culture of Nature: North American landscape from Disney to the Exxon Valdez*. Between the Lines, 1991.

[2] S. P. Anson and D. Cummings, 'The First Space War: The contribution of satellites to the Gulf War', *RUSI J.*, vol. 136, no. 4, pp. 45–53, Dec. 1991.

[3] S. Lambakis, 'Space Control in Desert Storm and Beyond', *Orbis*, vol. 39, no. 3, pp. 417–433, Jun. 1995.

[4] Y. Fukushima, 'Debates over the Military Value of Outer Space in the Past, Present and the Future: Drawing on Space Power Theory in the US', *NIDS J. Def. Secur.*, pp. 35–48, 2013.

[5] L. Greenemeier, 'GPS and the World's First "Space War"', *Scientific American*, 8 Feb 2016. [Online]. Available: https://www.scientificamerican.com/article/gps-and-the-world-s-first-space-war/. [Accessed: 17-Dec-2018].

[6] T. Brown, 'Space and the Sea: Strategic considerations for the commons', *Astropolitics*, vol. 10, no. 3, pp. 234–247, Dec. 2012.

[7] B. E. Bowen, 'British Strategy and Outer Space: A missing link?," *Br. J. Polit. Int. Relat.*, vol. 20, no. 2, pp. 323–340, May 2018.

[8] D. Paikowsky, *The Power of the Space Club*. Cambridge University Press, 2017.

[9] C. B. Halstead, 'The Ultimate High Ground - U.S. intersector cooperation in outer space', *J. Air Law Commer.*, vol. 81, pp. 595–610, 2016.

[10] K. Pollpeter, 'Space, the new domain: Space operations and Chinese military reforms', *J. Strateg. Stud.*, vol. 39, no. 5–6, pp. 709–727, Sep. 2016.

[11] D. Koplow, 'ASAT-isfaction: Customary international law and the regulation of anti-satellite weapons', *Georget. Law Fac. Publ. Works*, Jan. 2009.

[12] D. E. Lupton, *On Space Warfare: A space power doctrine*. PN, 1988.

[13] Chatham House, 'Making the Connection: The future of cyber and space', London, International Security Workshop Seminar, Jan. 2013.

[14] D. J. St. James, 'The Legality of Antisatellites' Recent Development', *Boston Coll. Int. Comp. Law Rev.*, vol. 3, pp. 467–494, 1980 1979.

[15] B. Jasani and C. Lee, *Countdown to Space War*. Taylor & Francis, 1984.

[16] S. J. Bruger, "Not Ready for the 'First Space War,' What about the second?' Naval War Coll Newport RI Dept of Operations, May 1993.

[17] J. E. Hyten, 'A sea of peace or a theater of war? Dealing with the inevitable conflict in space', *Air Space Power J.*, vol. 16, no. 3, p. 78, 2002.

[18] V. Anantatmula, ‘U.S. Initiative to Place Weapons in Space: The catalyst for a space-based arms race with China and Russia’, *Astropolitics*, vol. 11, no. 3, pp. 132–155, Sep. 2013.

[19] M. A. Gubrud, ‘Chinese and US Kinetic Energy Space Weapons and Arms Control’, *Asian Perspect*., vol. 35, no. 4, pp. 617–641, 2011.

[20] T. Harrison, K. Johnson, and T. Roberts, ‘Space Threat Assessment 2018’, 2018.

[21] N. Tannenwald, ‘Law versus Power on the High Frontier: The case for a rule-based regime for outer space’, *Yale J. Int. Law*, vol. 29, pp. 363–422, 2004.

[22] R. Handberg, ‘Is Space War Imminent? Exploring the possibility’, *Comp. Strategy*, vol. 36, no. 5, pp. 413–425, Oct. 2017.

[23] P. Stares, ‘Space and US National Security’, *J. Strateg. Stud*., vol. 6, no. 4, pp. 31–48, Dec. 1983.

[24] S. Freeland, ‘Peaceful Purposes - Governing the military uses of outer space’, *Eur. J. Law Reform*, vol. 18, pp. 35–51, 2016.

[25] J. A. Urban, ‘Soft Law: The key to security in a globalized outer space’, *Transp. Law J*., vol. 43, pp. 33–50, 2016.

[26] P. Meyer, ‘Dark Forces Awaken: The prospects for cooperative space security’, *Nonproliferation Rev*., vol. 23, no. 3–4, pp. 495–503, Jul. 2016.

[27] F. Grimal and J. Sundaram, ‘The Incremental Militarization of Outer Space: A threshold analysis’, *Chin. J. Int. Law*, vol. 17, no. 1, pp. 45–72, Mar. 2018.

[28] B. Gill and M. Kleiber, ‘China’s Space Odyssey: What the antisatellite test reveals about decision-making in Beijing’, *Foreign Aff.*, vol. 86, no. 3, pp. 2–6, 2007.

[29] J. Moltz, *The Politics of Space Security: Strategic restraint and the pursuit of national interests, Second edition*. Redwood City, United States: Stanford University Press, 2014.

[30] C. Baylon, ‘Challenges at the Intersection of Cyber Security and Space Security’, *Int. Secur.*, 2014.

[31] Z. Shabbir and A. Sarosh, ‘Counterspace Operations and Nascent Space Powers’, *Astropolitics*, vol. 16, no. 2, pp. 119–140, Aug. 2018.

[32] B. L. Triezenberg, ‘Deterring Space War: An exploratory analysis incorporating prospect theory into a game theoretic model of space warfare’, Rand Corporation, Santa Monica, CA, Product Page, 2017.

[33] M. Levine, ‘Russia Tops List of Countries that could Launch Cyberattacks on US’, *ABC News*, 19-May-2017. [Online]. Available: https://abcnews.go.com/US/russia-tops-list-100-countries-launch-cyberattacks-us/story?id=47487188. [Accessed: 18-Dec-2018].

[34] M. Smeets, ‘The Strategic Promise of Offensive Cyber Operations’, *Strateg. Stud. Q*., vol. 12, no. 3, pp. 90–113, 2018.

[35] J. Sigholm, ‘Non-State Actors in Cyberspace Operations’, *J. Mil. Stud.*, vol. 4, no. 1, pp. 1–37, Dec. 2013.

[36] A. Grigsby, ‘The End of Cyber Norms’, *Survival*, vol. 59, no. 6, pp. 109–122, 2017.

[37] T. Rid and B. Buchanan, ‘Attributing Cyber Attacks’, *J. Strateg. Stud*., vol. 38, no. 1–2, pp. 4–37, Jan. 2015.

[38] J. R. Lindsay, ‘Tipping the Scales: The attribution problem and the feasibility of deterrence against cyberattack’, *J. Cybersecurity*, vol. 1, no. 1, pp. 53–67, Sep. 2015.

[39] N. Tsagourias, ‘Cyber attacks, self-defence and the problem of attribution’, *J. Confl. Secur. Law*, vol. 17, no. 2, pp. 229–244, Jul. 2012.

[40] B. I. Koerner, ‘Inside the OPM Hack, the cyberattack that shocked the US government’, *Wired*, 23-Oct-2016.

[41] NASA, ‘ARES: Orbital Debris Program Office Frequently Asked Questions’, 2018. [Online]. Available: https://orbitaldebris.jsc.nasa.gov/faq.html#3. [Accessed: 10-Dec-2018].

[42] L. David, ‘Russian Satellite Hit by Debris from Chinese Anti-Satellite Test’, *Space.com*, 08-Mar-2013. [Online]. Available: https://www.space.com/20138-russian-satellite-chinese-space-junk.html. [Accessed: 10-Dec-2018].

[43] D. Mosher, ‘The US Government Logged 308,984 Potential Space-Junk Collisions in 2017 — and the problem could get much worse’, *Business Insider*, 15-Apr-2018. [Online]. Available: https://www.businessinsider.com/space-junk-collision-statistics-government-tracking-2017-2018-4. [Accessed: 10-Dec-2018].

[44] B. Weeden, ‘Global Space Situational Awareness Sensors’, Sep. 2010.

[45] B. Lal, A. Balakrishnan, B. Caldwell, R. Buenconsejo, and S. Carioscia, ‘Global Trends in Space Situational Awareness and Space Traffic Management’, Apr. 2018.

[46] D. A. Vallado and J. D. Griesbach, ‘Simulating Space Surveillance Networks’, Paper AAS 11-580 presented at the AAS/AIAA Astrodynamics Specialist Conference. Jul. 2011.

[47] D. Bird, ‘Sharing Space Situational Awareness Data’, Strategic Command Offutt AFB NE, Sep. 2010.

[48] JFSCC, ‘SSA Sharing & Orbital Data Requests’, *Space-Track.org*, 2018. [Online]. Available: https://www.space-track.org/documentation#/odr. [Accessed: 10-Dec-2018].

[49] N. Shah, M. Richards, D. Broniatowski, J. Laracy, P. Springmann, and D. Hastings, ‘System of Systems Architecture: The case of space situational awareness’, in *AIAA Space 2007 Conference & Exposition*, 0 vols., American Institute of Aeronautics and Astronautics, 2007.

[50] ai-solutions, *FreeFlyer® Software*. 2018.

[51] C. Früh and T. Schildknecht, ‘Accuracy of Two-Line-Element Data for Geostationary and High-Eccentricity Orbits’, *J. Guid. Control Dyn*., vol. 35, no. 5, pp. 1483–1491, 2012.

[52] NASA, ‘Human Space Flight (HSF) - Realtime data’, *NASA SkyWatch*, 2011. [Online]. Available: https://spaceflight.nasa.gov/realdata/sightings/SSapplications/Post/JavaSSOP/SSOP_Help/tle_def.html. [Accessed: 20-Dec-2018].

[53] Air Force Space Command, ‘Astrodynamic Standards Software’, *Air Force Space Command*, 22 Mar 2017. [Online]. Available: https://www.afspc.af.mil/About-Us/Fact-Sheets/Display/Article/249006/astrodynamic-standards-software/. [Accessed: 11-Dec-2018].

[54] F. Johnson, ‘1 Million Subscribers Connected: Iridium helps prevent shark attacks while protecting local ecosystems’, *Iridium Satellite Communications*, 18 Jun. 2018.

[55] P. Selding, U.S. Defense Agency Encourages Allied Nations to Join Unlimited-Use Iridium Program’, *SpaceNews.com*, 11 Nov. 2016. [Online]. Available: https://spacenews.com/u-s-defense-agency-encourages-allied-nations-to-join-unlimited-use-iridium-program/. [Accessed: 14-Dec-2018].