EasyChair Preprint

№ 9839

The Vulnerabilities Less Exploited: Cyberattacks on End-of-Life Satellites

Frank Lee and Gregory Falco

March 7, 2023

The Vulnerabilities Less Exploited: Cyberattacks on End-of-Life Satellites

Frank Lee
Johns Hopkins University
flee39@jhu.edu

Gregory Falco
Johns Hopkins University
falco@jhu.edu

***Abstract*—End-of-life (EOL) satellites are space assets that have completed their primary mission. Due to their loss in commercial or scientific priority, EOL satellites are often left in place by operators for an extended period, instead of being decommissioned in a timely manner to free up high-value orbits. This period of inactivity exposes EOL satellites to a lower level of operator vigilance, and therefore, higher level of cyberattack risk. With the recent growth in space activities, this paper estimates there will be up to 5,000 inactive satellites in low Earth orbit (LEO) within 5 years, magnifying the space cyber risks and resulting space sustainability challenges. To bolster space cybersecurity, the authors illuminate unique attack vectors against EOL satellites, as well as policy and technical mitigation measures. When part of a constellation, the vulnerability of an EOL satellite has even bigger implications, where a threat actor may use the secondary asset to target primary assets. Ultimately, the active management of EOL satellites is significant for a secure and sustainable LEO infrastructure.**

I. Introduction

More than ever, space has increased its strategic importance as critical infrastructure for civil, military, and commercial activities. The need to protect space has been acknowledged across the international community, including orbital debris management for the physical security and sustainability of high-value orbits such as LEO. This paper discusses the cybersecurity layer of space sustainability by uncovering the often overlooked vulnerability of end-of-life (EOL) satellites.

EOL satellites are space assets that have ended their primary mission. Their operators are then requested, but not enforced, to decommission or deorbit these assets, in order to free up high-value orbits. Technically, NASA has set a maximum guideline of 25 years before an EOL satellite has to start its post-mission deorbiting process [1]. Since these satellites have lost most of their remaining commercial or scientific value, any extended time period after primary mission and before their final deorbit can often face the least amount of vigilance by the satellite operators.

Given EOL satellites are often still operational, if left in their original orbits, cyber threat actors may seek to corrupt or disable these assets, potentially blocking high-value orbits. In a more extreme scenario, attackers can gain access to the EOL satellites' propulsion or power subsystems and intentionally colliding with debris or other satellites, rendering certain orbits inaccessible for decades to come. Thus, attacks against EOL satellites may be be particularly harmful for space access and space sustainability.

This paper aims to highlight unique attack vectors for EOL satellites. Furthermore, both policy and technical mitigation measures are discussed with future work proposed to reduce the cyber risk to EOL satellites, as well as its broader impact on space sustainability.

II. Prior Art

A. EOL Satellite Landscape in LEO

The extent of the EOL satellite problem can be quantified by the number of inactive satellites in LEO, given its importance as a high-value orbit. While the number of active satellites in LEO is readily available in open-source databases, the number of inactive satellites requires some cross-referencing of multiple resources and estimations.

The first reference point derives from Geospatial World [2], a technology researcher for various sectors including the space industry. In 2021, Geospatial World reports 6,542 total Earth orbiting satellites, including 3,372 active satellites and 3,170 inactive satellites. Given that 90% of satellites are estimated to be in LEO, an extrapolation can place the number of inactive satellites to be around 2,853. However, the methodology used in the article is not readily available, and thus, other sources are cross-referenced.

The second reference point derives from the Union of Concerned Scientists (UCS) [3] and the University of Texas at Austin's Astriagraph [4] databases. The UCS database reports over 3,000 active satellites in LEO today. Astriagraph is a visualization tool that compiles active and inactive space objects around Earth from multiple private and public data sources. While it allows filtering to visualize only active and inactive satellites in LEO, the tool unfortunately does not easily allow raw data exports of the exact number of various objects. Thus, Figure 1 attempts to visually estimate about an 1:1 to 3:2 active to inactive satellites ratio in LEO as demonstrated by Astriagraph. By combining the UCS and the Astriagraph databases, this paper extrapolates the number of inactive satellites in LEO to be 2,000 to 3,000 satellites, which

Workshop on Security of Space and Satellite Systems (SpaceSec) 2023
27 February 2023, San Diego, CA, USA
ISBN 1-891562-89-4
https://dx.doi.org/10.14722/spacesec.2023.234958
www.ndss-symposium.org

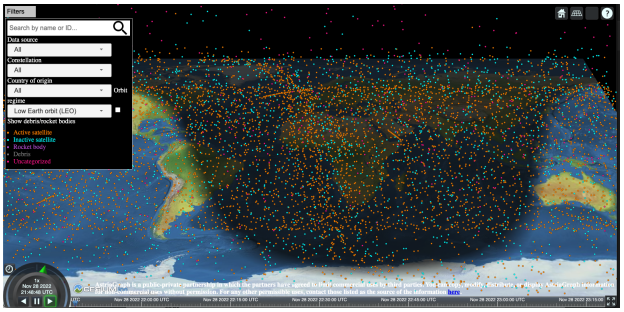

Fig. 1: Astriagraph active and inactive LEO satellites [4]

is within range to the Geospatial World estimation of 2,853 inactive satellites. While many inactive satellites are older with depleted fuel tanks, the recent growth in launches presents an emergent EOL satellite challenge.

The final reference point is a projection forward. BIS Research estimates over 43,000 satellites are to be launched between 2022 to 2032 into LEO by organizations globally [5][6]. Assuming a 5-year mission life, this can add 1,000 to 2,000 inactive satellites in the next 5 years. Cross-referencing all data sources, there are currently 2,000 to 3,000 inactive satellites in LEO, with a potential increase of up to 2x in the total number of inactive satellites within 5 years.

B. EOL Satellite Deorbiting Options in LEO

Towards the end of their useful life, satellites in LEO (altitude of 2,000 km or less) can deorbit from their original orbit by either descending into a decay orbit or raising to a graveyard orbit. The first option is to position the satellite into a lower altitude for orbital decay, starting its journey to atmospheric reentry and burn up. At altitudes less than 200 km, the Earth's atmosphere becomes very dense, allowing the EOL satellite's orbit to exponentially decay in altitude due to drag upon its body. Upon reentry, most satellites are designed to burn up with the atmospheric friction. Depending on the satellite's final altitude set for orbital decay, the timeline to reach its atmospheric burn up varies. For example, if the decay orbit starts at 400 km, the lifetime can last as much as 1 year. At a decay orbit of 200 km, the lifetime can last about a day [7]. For LEO satellites with an original orbit of 1,400 km or higher, there is a second option to raise the altitude to a graveyard orbit between LEO and the geostationary orbit (GEO) at 2,000 km to 35,586 km [8].

For either disposal option, once set in a decay orbit or a graveyard orbit, best practices recommend placing the spacecraft in passivity mode, which includes depressurizing the fuel tank and discharging the battery. However, in practice, there is a lengthy time delay between EOL and passivation, presenting an opportunity for attackers.

C. Case Studies

A main theme to the increased vulnerability of an EOL satellite is the operator's tendency to deprioritize the satellite after completing its primary mission. The period between the end of a satellite's primary mission and its eventual deorbiting is the most vulnerable time for possible cyberattacks due to a lack of vigilance and deprioritization of resources. While there are no public incidents, these hypothetical challenges have been openly discussed. Two case studies are presented to explore what typically happens upon mission conclusion.

Iridium: During the 2019 Orbital Debris Conference [9], Iridium presented a paper on the deorbiting of its 66-satellite B1 constellation. Iridium had replaced its older B1 constellation with its newly launched NEXT constellation. Thus, it had a unique opportunity to become the first company to deorbit a large constellation. In December 2019, Iridium announced that the company had placed its final satellite into passivity mode on a decay orbit. However, the conference paper and another SpaceNews source [10] revealed that it took about 2-3 years between the end of service for the B1 constellation and the end of its deorbiting program. Iridium had used that extended period to obtain approval for a deorbiting plan with external entities, including the Combined Space Operations Center (CSpOC) and NASA. While within NASA's 25-year deorbiting guideline, 2-3 years is a considerable time period for functional, but deprioritized assets to remain in orbit.

SiriusXM: In December 2020, the SiriusXM's SXM-7 satellite failed after orbital insertion. Details about the primary payload failure were not released publicly. Initially, SXM-7 inserted into GEO around 36,000 km. As of December 2022, the satellite can still be tracked around 35,790 km. This altitude is below the GEO graveyard of 36,300 km according to the European Space Agency's guideline [13]. The operator decided to leave SXM-7 in orbit instead of raising the satellite into the GEO graveyard for disposal. Numerous media outlets reported that SXM-7 was declared a total loss, with SiriusXM filing a $225 million insurance claim [11]. The public did not know why SXM-7 was left in orbit until recently. On November 29, 2022, SiriusXM's vice president of satellite operations and terrestrial engineering reported on SpaceNews that SXM-7 has a secondary payload, but declined to detail its service [12]. In this example, given its failure and subsequent insurance claim, monitoring the primary payload is unlikely the mission priority. While the satellite is still operating with its secondary payload, should they not be segmented, the primary payload's EOL may serve as an attack vector to the secondary payload or the bus. This is especially true for hosted payload architectures, if not secured properly.

III. Attacking EOL Satellites

A. Established Attack Vectors Against Satellites

While telecommand authentication enhances security, operators face tradeoffs between security risk and performance costs from encryption delays [17]. Furthermore, the Aerospace Corporation's SPARTA framework offers tactics, techniques and procedures (TTPs) that a threat actor may wage against a satellite. As an example, SPARTA demonstrates how a man-in-the-middle attack can be accomplished along with countermeasures [18]. Since EOL satellites are subject to many

Position	EE&CO FTE	Nominal FTE	Mature FTE	Shift (hr/day)
Operations Manager	1	0.5	0.1	8/5
Spacecraft Controller	2	0.9	0.1	8/5, 8/7 for EE&CO
Ground Controller	1	0.1	0.1	8/5
Mission Planner	2	1	1	8/5
Data Manager	1	0.5	0.1	8/5
S/C Analyst	4	0.5	0.1	8/5, 8/7 for EE&CO
Software Analyst	2	0.5	0.1	8/5, 8/7 for EE&CO
Orbit Analyst	1	0.5	0.1	8/5
Total	14	4.5	1.7	

TABLE I: Staffing for a small satellite mission [14]

of the same TTPs compared with an active satellite, this paper focuses on the attack vectors unique to EOL satellites.

B. Unique Attack Vectors Against EOL Satellites

Exploiting Reduced Staffing and Secondary Status: Several unique attack vectors of EOL satellites hinge on the reduced staffing that commonly manifests at the end of a primary mission. Given that the satellites no longer have remaining commercial or scientific value, the period right after the completion of mission can face the least amount of vigilance by the satellite operators. Using an automated small satellite mission as an example, the textbook *Space Mission Planning: The New SMAD* illustrates with Table I that the staffing level towards the end of a mission is less than 40% of the nominal mission phase, or at most 10% of the Engineering Evaluation and Checkout (EE&CO) phase after orbit insertion [14]. While automation can help to manage EOL operations, reduced staffing poses operational challenges to analyzing anomalies.

Strategically, space organizations must prioritize its resources accordingly for missions with the highest profitability or scientific value, resulting in an optimization for the best possible gains similar to managing a financial portfolio. This priority disparity can create a timing opportunity for attackers to target EOL satellites, while the organization is focusing on assets operating in higher value missions.

Exploiting Mission Fatigue and Attrition: Fatigue and morale factors are both qualitative measurements to be considered during a mission life cycle [14]. At the completion of a primary mission, both factors can rate poorly for operators that must manage EOL satellites versus other higher organizational priorities. During a cyberattack, should the threat actor leave traces of their activity on the spacecraft log files, the operators may disregard the anomaly both due to their own mission fatigue and underestimating the attractiveness of EOL satellites to threat actors.

Furthermore, operators may switch roles in between mission assignments or leave the organization altogether as common with employee attrition at the completion of a major milestone. With weak access control, this scenario can lend itself to increasing attack risk [15]. For example, at the end of a primary mission, Operator X moves onto a new mission team. Given poor access controls, this operator's access profile may still function for commanding an EOL satellite, creating a vulnerable point for attack.

Exploiting Unpatched Software: As a parallel industry, the FBI Cyber Division has issued guidance on protecting medical devices by managing software upgrades with manufacturers to consistently close any unpatched exploits [16]. For spacecrafts, any software maintenance program should extend to EOL satellites, which will require any software releases to be backwards compatible and may incur additional ground station costs to up-link software updates. Otherwise, satellite operators may find themselves managing a portfolio of space assets with attack surfaces of varying degrees that grow more difficult to mitigate over time.

Exploiting EOL Satellite Cross-Links: While a threat actor can render an EOL satellite into a permanent roadblock within a high-value orbit, another unique attack vector rides on gaining access to the less defended EOL satellite first, for the sole purpose of accessing a higher-value asset within the same constellation. The SPARTA framework discusses the attack of a space asset via cross-link of a compromised neighbor satellite [18]. Thus, if the operator failed to exclude an EOL satellite from the constellation cross-link, an attacker can first take command of the EOL satellite, prior to compromising a primary space asset by sending malicious commands. When part of a constellation, this vulnerability has even bigger implications beyond just the EOL satellite, especially with the growing number of large constellations [19].

IV. Attack Mitigation for EOL Satellites

A. Policy Mitigation

Policy as a vehicle for cyber threat mitigation measures against EOL satellite attacks may benefit from policy intending to improve orbital debris cleanup. Fewer inactive orbital objects translate to fewer attack opportunities for EOL satellites. Since 2022, FCC has considered setting a 5-year deadline for deorbiting satellites, shortening NASA's previous deorbiting guideline of 25 years [20]. While there are many challenges to implement this proposal, including operators having to potentially shorten their satellite asset lifespan, this requirement may force operators to plan EOL procedures carefully and be timely about the eventual disposal of their space assets. Furthermore, also in 2022, the Senate passed a bill mandating NASA to implement a program that identifies and manages orbital debris, which poses the greatest immediate risk to the sustainability of high-value orbits [21]. However, this bill has yet to define the requirements of such a program, nor has the bill passed Congress.

To further establish a governance tool for orbit operators and policy makers, A.V. Gheorghe and D.E. Yuchnovicz proposed a cadastre that evaluates the risk factor for debris collision by modeling debris density at different orbit altitudes [22]. The altitude band with the highest risk puts the orbit at an

unacceptable operational risk status. Tools like this can help both policy makers and operators design missions with the EOL in mind, ensuring the proper margins for propulsion and power budgets for both debris avoidance and timely disposal.

B. Technical Mitigation

Deorbiting as a Service: In general, the unique attack vectors to an EOL satellite can best be mitigated by a timely, efficient satellite deorbiting process, removing itself as a target post-mission. The mission life cycle from orbital insertion to operations to deorbiting can be segmented and managed by different third-party operators. A deorbiting as a service company can offer EOL satellite service operations. This may include a remote access capability, allowing mission operators to securely sign over satellites to the deorbiting company to manage, monitor, and deorbit at EOL. Given the deorbiting company specializes in EOL services, the third-party operator can build process efficiencies, reducing operator cost.

Using the self-driving trucking industry as an analogy, while the majority of ventures focuses on general cargo long-hauls, Gatik is an AI trucking startup that specializes in the short-hauls between a retailer and its warehouse hubs [25]. These short-haul routes are more predictable and routine, allowing Gatik to focus the development of its services with a more confined set of variables, thereby reducing costs for end users. The development of services and technology for deorbiting can benefit from a similar outsourced approach to EOL services.

Digital Sanitization of EOL Satellites: For general computers and servers reaching EOL, the National Institute of Standards and Technology (NIST) has published guidelines for IT asset disposal. Specifically, NIST advocates for digital sanitization techniques that either overwrite sensitive data or render media obsolete, in order to protect against attackers from obtaining unauthorized access to systems at EOL [26]. Similarly, EOL satellites can benefit from such digital sanitization by overwriting their mission software with an EOL flight software limited to performing only final disposal maneuvers. This approach helps to mitigate the vulnerability of not patching EOL satellites with the latest mission flight software. For example, while not a complete digital sanitization procedure, Iridium updated its satellites with a final flight software with deorbiting and passivation sequences, which may have removed the mission flight software [9].

Autonomous Decommissioning: In LEO, the decommissioning of an EOL satellite can be broadly segmented into three main phases. First, the satellite needs to deorbit from its original altitude by descending into a decay orbit or raising to a graveyard orbit. Second, the satellite needs to be placed in passivity mode, depressurizing its fuel tanks and discharging its batteries. Finally, the satellite either burns up upon reentering atmosphere from a decay orbit, or sits in permanent storage in the graveyard orbit. The recent development of spacecraft tracking and rendezvous technologies [23][24] can help automate this decommissioning process. Post-mission, EOL satellites can be placed in a cyber-safe mode for automated decommissioning. Any command to intervene or control the spacecraft is disallowed, unless a secured authentication is approved for operators to restore the spacecraft back to operating mode. The cyber-safe mode enables the EOL satellite to safely and automatically change trajectory into a decay orbit or a graveyard orbit, implement passivity procedures, and perform final digital sanitization. This autonomous decommissioning capability allows the timely disposal of EOL satellites, while mitigating any cyberattack risks throughout the process.

V. Discussion

Space sustainability challenges are at an unprecedented state of visibility for the public and international community; however, the digital concerns relating to the ever-increasing volume of decommissioned assets is being largely overlooked. As governments and the international NGOs begin to consider solutions to minimize the impact of EOL satellites on physical orbits, they should simultaneously develop protocol to digitally decommission space vehicles. As described, there are unique aspects of EOL systems, which can be exploited to wreak havoc on an already challenging space operating environment. Given the United States is at the precipice of introducing new policy relating to ”In-Space Authorization and Supervision,” it will be critical to integrate EOL cyber considerations into such a framework. Future work spans policy and technical domains. Policy guidance should be written to inform cyber EOL procedures that can be practically regulated and monitored. Further technical work is required to develop tools to minimize technical risk for EOL satellites such as cyber-safe mode or developing a means to autonomously decommission digital mission assets, once they have achieved their objective.

VI. Conclusion

While EOL satellites may not be perceived as desirable targets, when overtaken and disabled, the results can be devastating for space sustainability. Within 5 years, given recent growth in space activities, this paper estimates up to 5,000 inactive satellites in LEO, furthering this concern.

In order to bolster defenses, this paper analyzes EOL satellites to have several unique attack vectors, including reduced staffing, lower priority status, mission fatigue, and inadequate software patching. With the growing number of large constellations, the vulnerability of EOL satellites can pose an attack vector via satellite cross-links.

In general, policy mitigation that enforces operators to clear high-value orbits in a timely manner at EOL will be effective at reducing the risk of cyber threats. Technical mitigation may include the development of deorbiting as a service, with a third-party operator taking over satellites at EOL to manage deorbiting tasks safely and efficiently. EOL satellites can also be protected by digitally sanitizing their flight software.

Ultimately, the international space community should move towards a future that includes post-mission autonomous decommissioning, where EOL satellites may be placed in a cyber-safe mode to automatically deorbit for disposal, implement passivity, and perform digital sanitization, while mitigating any cyberattack risk throughout the process.

ACKNOWLEDGEMENT

The authors would like to thank all the efforts from commercial, civil, and military organizations helping to manage and clear orbital debris from near Earth orbits. Space sustainability has inspired the ideas behind this paper by highlighting a shared objective from the field of space cybersecurity.

REFERENCES

[1] "13.0 Deorbit Systems," *NASA - https://www.nasa.gov/smallsat-institute/sst-soa/deorbit-systems*

[2] N. Mohanta, "How many satellites are orbiting the Earth in 2021," *Geospatial World - https://www.geospatialworld.net/blogs/how-many-satellites-are-orbiting-the-earth-in-2021/*

[3] "UCS Satellite Database," *Union of Concerned Scientists - https://www.ucsusa.org/resources/satellite-database*

[4] *The University of Texas at Austin, Astriagraph - http://astria.tacc.utexas.edu/AstriaGraph/*

[5] "Global Space Situational Awareness Services Market Report 2022-2032," *BIS Research - https://www.globenewswire.com/en/news-release/2022/08/08/2493644/28124/en/Global-Space-Situational-Awareness-Services-Market-Report-2022-2032-Market-to-be-Driven-by-the-Increasing-Number-of-Small-Satellite-Constellations-in-the-Low-Earth-Orbit-LEO.html*

[6] "Annual number of objects launched into space," *Our World in Data - https://ourworldindata.org/grapher/yearly-number-of-objects-launched-into-outer-space*

[7] "Satellite Orbital Lifetime," *Space Academy - https://www.spaceacademy.net.au/watch/debris/orblife.htm*

[8] S.M. Hull, J.R. Wertz, D.F. Everett, and J.J. Puschell (2018) *Space Mission Engineering: The New SMAD*, Chapter 30 End of Mission Considerations, pp. 937 - 946, Space Technology Library.

[9] W. Everetts, K. Rock, and M. Iovanov, "Iridium Deorbit Strategy, Execution, and Results," *First International Orbital Debris Conference 2019*

[10] C. Henry, "Iridium starting to deorbit legacy satellites as Next constellation comes online," *Space News - https://spacenews.com/iridium-starting-to-deorbit-legacy-satellites-as-next-constellation-comes-online/*

[11] D. Todd, "SXM-7 payload failure is a bad start to the year for space insurance market," *Seradata - https://www.seradata.com/sxm-7-payload-failure-is-a-bad-start-for-space-insurance-market/*

[12] J. Rainbow, "SiriusXM orders pair of satellites to expand in Canada and Alaska," *Space News - https://spacenews.com/siriusxm-orders-pair-of-satellites-to-expand-in-canada-and-alaska/*

[13] "Where old satellites go to die," *European Organisation for the Exploitation of Meteorological Satellites - https://phys.org/news/2017-04-satellites-die.html*

[14] T.C. Sorensen, J.R. Wertz, D.F. Everett, and J.J. Puschell (2018) *Space Mission Engineering: The New SMAD*, Chapter 29 Mission Operations, pp. 903 - 934, Space Technology Library.

[15] "Weak Security Controls and Practices Routinely Exploited for Initial Access," *Cybersecurity & Infrastructure Security Agency - https://www.cisa.gov/uscert/ncas/alerts/aa22-137a*

[16] "Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities," *Federal Bureau of Investigation, Cyber Division*, September 12, 2022.

[17] C. Maple et al., "The Impact of Message Encryption on Teleoperation for Space Applications," 2022 IEEE Aerospace Conference (AERO), Big Sky, MT, USA, 2022, pp. 1-10, doi: 10.1109/AERO53065.2022.9843424.

[18] "Space Attack Research & Tactic Analysis (SPARTA)," *The Aerospace Corporation - https://sparta.aerospace.org/*

[19] C. Daehnick, I. Klinghoffer, B, Maritz, and B. Wiseman, "Large LEO satellite constellations: Will it be different this time," *McKinsey & Company - https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/large-leo-satellite-constellations-will-it-be-different-this-time*

[20] J. Foust, "FCC to Set 5-Year Deadline for Deorbiting LEO Satellites," *SpaceNews - https://spacenews.com/fcc-to-set-five-year-deadline-for-deorbiting-leo-satellites/*

[21] J. Foust, "Senate passes orbit debris cleanup bill," *SpaceNews - https://spacenews.com/senate-passes-orbit-debris-cleanup-bill/*

[22] A.V. Gheorghe and D.E. Yuchnovicz, "The Space Infrastructure Vulnerability Cadastre: Orbital Debris Critical Loads," *International Journal of Disaster Risk Science* volume 6, 359–371 (2015).

[23] "Our Life Extension Services: Mission Extension Vehicle," *Nothrop Grumman - https://www.northropgrumman.com/space/space-logistics-services/*

[24] A. Alamalhodaei, "Astroscale successfully demos in-space capture-and-release system to clear orbital debris," *TechCrunch - https://techcrunch.com/2021/08/25/astroscale-successfully-demos-in-space-capture-and-release-system-to-clear-orbital-debris/*

[25] "Gatik and Walmart Achieve Fully Driverless Deliveries in a First for Autonomous Trucking Industry Worldwide" *Business Wire - https://www.businesswire.com/news/home/20211108005409/en/Gatik-and-Walmart-Achieve-Fully-Driverless-Deliveries-in-a-First-for-Autonomous-Trucking-Industry-Worldwide*

[26] R. Kissel, A. Regenscheid, M. Scholl, and K. Stine, "Guidelines for Media Sanitization," *NIST Special Publication* 800-88, Revision 1.