Monitoring of rendezvous and proximity operations with SST and SDA techniques combination

Jaime Serrano[(1)], Ángel Gallego[(1)], Álvaro Martínez[(1)], David Moreno[(1)]

[(1)] GMV, Calle Isaac Newton 11, Tres Cantos, 28670, Spain, jaserrano@gmv.com, agtorrego@gmv.com, amartinez.l@gmv.com, dmespinosa@gmv.com

1. INTRODUCTION

In the modern era, the number of satellites and space systems providing services, information, and capabilities to Earth has reached unprecedented levels. While many of these systems are intended for civilian use and are managed by private companies rather than governments, they also play a vital role in national security. These civilian and commercial space systems are increasingly becoming targets for foreign adversaries, facing escalating threats such as cyber-attacks and espionage. Seven years ago, the Center for Strategic and International Studies (CSIS) of the US initiated the publication of threat assessments through the Aerospace Security Project [1]. This initiative underscores the recognition that space has long been considered a strategic domain where nations can deploy their defense strategies.

Given the critical services and capabilities that space systems offer for national and economic security, the field of Space Domain Awareness (SDA) is undergoing significant and rapid evolution. This evolution is driven by the emergence of new technological challenges each year. The utilization of space has transformed from being the domain of a few select organizations to a landscape where numerous private companies, individuals, and a growing number of nations strategize to pursue various interests using space as the primary domain. This shift has resulted in the launch of thousands of objects into space, serving a wide array of purposes. These Resident Space Objects (RSOs) are tracked and catalogued using Space Surveillance and Tracking (SST) techniques. The SST field is also evolving swiftly to adapt to the new scenario presented by the increasing number of RSOs. This rapid evolution is essential to ensure the continued safety and functionality of space systems amidst the growing complexity and threats in the space environment.

In this scenario, capabilities in the SDA domain must evolve to effectively manage intentional threats. One prominent example of such threats includes the Rendezvous and Proximity Operations (RPO) conducted by inspector satellites targeting assets of strategic interest. Inspector satellites are specialized spacecraft designed to approach and interact with other satellites. They perform RPOs to spy or potentially disrupt the targeted satellites. Although RPO operations can be used for legitimate purposes, such as maintenance and repair, they pose significant risks if used for espionage or sabotage. As a result, enhancing SDA capabilities to monitor and respond to RPOs is crucial for maintaining the security and integrity of space assets.

To demonstrate the presence of these threats in the current space environment, consider the behavior of satellites Olymp-K (Luch) and Olymp-K-2 (Luch-5X), launched in 2014 and 2023, respectively. These satellites have been observed executing close approaches to other satellites in the geostationary belt, without clear intentions. These maneuvers, known as RPOs, involve one satellite approaching another closely enough to potentially gather intelligence or disrupt its operations. In 2022, Cosmos-2558 closely approached USA-326, likely capturing images or collecting signals intelligence. These activities highlight the escalating risks in space, where the motives behind such close encounters remain uncertain and potentially hostile.

This is proof of the importance of detecting and monitoring RPOs as a pillar for preserving security in space within the context of SDA complemented by the safety and sustainability efforts supported by the SST domain. This paper provides an overview of several cases of RPOs, the study of the behavior of inspector satellites and the methodologies used within SDA to handle them. Additionally, it analyzes the combined use of typical SST capabilities to prevent and mitigate the impact of these events. Finally, the study presents results from the analysis of various scenarios, aiming to determine the typical parameters governing intentional RPO approaches. These parameters include anticipation in detection time and the possibility of taking reactive measures. By optimizing these times and improving characterization through appropriate use of proposed methodologies, we enhance our ability to manage RPOs effectively.

A Close Proximity Operation (CPO) involves the controlled approach of one satellite—the inspector satellite—to another, known as the asset of interest. The inspector satellite trajectory allow it to come close to its target without colliding. If the approach continues until contact is made, it is considered a rendezvous. Detecting such events requires prior knowledge of the trajectories of the involved satellites. This is where SST capabilities combine with SDA, leveraging cataloging and maneuver detection based on sensor networks. Monitoring of the specific event is triggered when the inspector crosses the boundaries of a security screening volume centered around the asset of interest.

The basic geometric analysis considers two volumes: the CPO zone, where close approaches are detected, and the CPO corridor, which is considered safe for rendezvous without collision risk. Determining whether a detected close approach poses a security or intelligence risk varies significantly for each case, necessitating in-depth analysis and information merging from multiple sources. By analyzing the relative positions of the two objects, we can distinguish between a fly-by and a co-orbital operation where both satellites share the same orbit. Rendezvous operations are detectable by assessing minimum expected distances, relative speeds, and the evolution of relative positions.

However, RPO analysis must go deeper. Combining it with characterization of the inspector satellite—based on its attitude law, evolution estimation, and other physical properties—provides insights into the satellite's purpose. Additionally, observing the inspector's pointing behavior (e.g., cameras, antennas, or jamming instruments) toward the asset of interest sheds light on the intention behind the proximity operation.

To mitigate the risk of being a target of a malicious RPO, we have studied how applying SDA techniques could provide operators with information of the threat posed by orbital neighbors of monitored assets. Analyzing the pattern of life of these objects may reveal the real nature of the satellites' mission and could provide information on maneuverable capabilities of suspicious satellites. Another direct source of information is the public catalogues. There is information such as the nominal position of active satellites, and when deviate from their usual orbit, it allows us to easily identify them as dangerous or suspicious. Other abnormal behaviors of orbital neighbors should be analyzed. Then, active satellites within reach of limited delta-velocity maneuvers should be closely tracked. Through a qualitative analysis of active satellites and their orbits, it is possible to create a risk map, which provides information on how close our assets could be to becoming a target of a malicious approach.

If a maneuver aligns with CPO characteristics, an alarm should be raised. Thus, our proposed way forward combines satellite characterization with RPO event detection, enhancing our understanding of these operations.

The actions to be performed when an intentional CPO is detected against one of our assets of interest are based in SST standard techniques: avoidance manoeuvres calculation, although there is the need for a deeper analysis of the consequences. If this is done sufficiently in advance, an avoidance plan can be put in place, either by modifying the Station Keeping (SK) plan or with a dedicated manoeuvre. The avoidance manoeuvre is geometrically calculated to exit the encounter with the inspector in a safe way. Moreover, a mitigation action can be performed by commanding a new attitude configuration for the asset of interest. This is, position it with a determined attitude concerning the inspector satellite, for example, to hide a part of interest or to perform a countermeasure. Out of the scope of the SST domain, SDA should consider the collocation of the inspector satellite in the same window as the asset of interest. This provides small numbers of possibilities to avoid the event.

Several simulated scenarios with a given population of active satellites have been analysed. In these scenarios, CPOs and non-intentional close trajectories between different satellites are included. The intentional malicious approaches are taken from real world cases extracted from [1]. The study of these cases allows to understand how to react to these cases and what will happen when one of the assets of interest is targeted by one of these threats. Within these scenarios, the possibilities of detecting the intentional RPOs have been studied. Results show that most events involving the inspector satellites are correctly determined as intentional when combining SST conjunction detection techniques and SDA characterization of the conjunction.

Moreover, additional methodologies, such as satellite qualitative characterization, neighbours' identification and pattern of life analysis on suspicious satellites notably improves threat characterization and how to react with a mitigation plan. The work performed also includes the analysis of how some inspector satellites behave and whether their operations can be predicted.

2. METHODOLOGY

2.1 Analysis Real Scenarios of CPOs

2.1.1 GEO: LUCH (40258) - INTELSAT 33e (41748): 16/09/21-01/02/22

The 28th of September 2021 *Luch* began to approach *Intelsat 33e*. As depicted in Fig. 1, *Luch* was situated at a lower longitude than Intelsat and performed a standard relocation manoeuvre in GEO.

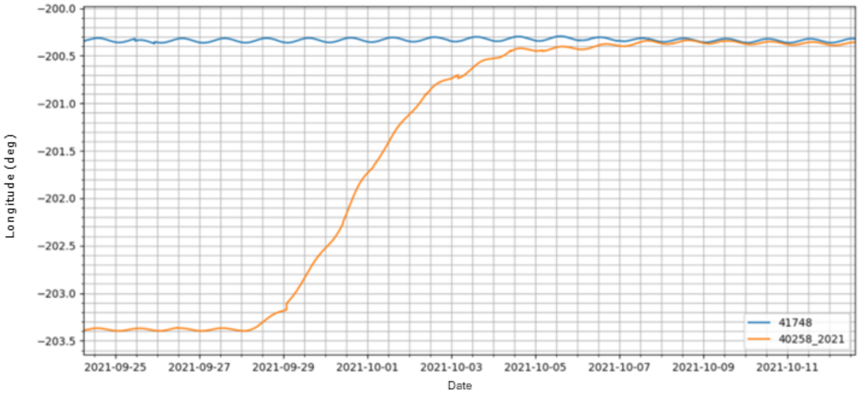

Fig. 1. Luch – Intelsat Longitude Evolution

Upon analysing the orbits of both satellites, it is noteworthy that Luch was already near the target satellite, with a difference of only 3 degrees in longitude. This suggests that the proximity operation to the INTELSAT satellite was premeditated, and monitoring of orbital neighbours is recommended in most instances.

The process of approach took approximately 5-6 days in this case before the satellites were less than 40km apart. The minimum distance achieved was only 6.5 km, and it was reached on 2021/10/08-23:57:06. The total duration of the Close Proximity Operation (CPO) between Luch and Intelsat was approximately 3 and a half months, from 05/10/2021 to 15/01/2022. During this period, the average distance between both satellites was 38.4km, with a standard deviation of 8.8km. This suggest that the *Luch* satellite position was a standard collocation in the same window where the *Intelsat 33e* was.

To reduce the longitude difference and approach the INTELSAT satellite, Luch had to undergo a relocation in GEO. The manoeuvres executed by the inspector satellite Luch have been analysed. However, this study has been performed using public data, and due to the availability of only one TLE each day, the information is limited, and the exact manoeuvres cannot be determined. It is only possible to observe the effects of the manoeuvres on the orbital parameters after each new TLE.

The relocation process followed the standard operations executed by GEO satellites for a circular relocation. Initially, with the TLE available on the 28th at midday, Luch began to reduce its semimajor axis while increasing its eccentricity, thereby entering an elliptical transfer orbit. Subsequently, on the 29th -30th, it transitioned into an almost circular orbit with a significantly lower eccentricity. Once the approach was halfway completed, Luch began the orbit raise to GEO position, returning to it on the 5th of October but this time at the same longitude as the target.

During these manoeuvres, the total delta V was estimated to be about 4.4 m/s, which can be calculated from the analytical computations of a Hoffman manoeuvre and considering the SMA of the intermediate circular orbit.

To determine how far in advance this RPO can be predicted, a method was employed where only the TLEs up to a certain date were used to see whether the encounter is correctly predicted or not. However, the limitations of this prediction stem from the fact that usually TLEs are only available once each day.

It was observed that, with a TLE for the 29th of September at 12 a.m., the conjunction is predicted accurately with a minimum distance of 57.5 km occurring on the 3rd of October at 14:00, which is relatively close to the first real encounter that took place on the 5th of October. If the encounter is predicted with the TLE of the previous day, a distance lower than 60km is estimated for the 20th of October, which is not admissible. Therefore, in this case, and considering that the first real encounter is on the 5th of October, it can be concluded that the RPO can be predicted with 6 days in advance.

In conclusion, to predict the encounter with relatively good accuracy, the inspector satellite should have entered the intermediate orbit for the relocation operation that has been described previously. Moreover, this can be seen from the fact that in this prediction, the radial distance between the two satellites in most cases is the same distance as the one from the intermediate orbit to the GEO orbit.

Finally, even before Luch starts its manoeuvres, an analysis was performed to see if an estimate of the approaching time could be obtained. This prediction was done analytically estimating the orbit of Luch as Hoffman transfer orbits. Using a obtained TLE before any manoeuvre had begun (the 26th of September), for a typical delta V for Luch (according to its usual manoeuvres) of 4 m/s, the estimated time results in 4.4 days, which is close to the 5-6 days of the real case. Similarly to before, the main difference comes from the fact that, in the real case, Luch does not perform a perfect Hoffman manoeuvre and in the last stages of the relocation it reduces its approaching rate.

2.1.2 GEO: USA 270 (41744) - SHINYAN 12 01/02 (50321/50322) 20/12/21 - 20/08/22

This case analysis delineates a distinct scenario involving the American satellite *USA 270* and the Chinese satellites *Shiyan 12-01* and *Shiyan 12-02*. Both satellites were launched towards the end of the year 2021 and had shared identical orbits until this intentional CPO performed by the American satellite. After a period where the Chinese satellites tried to escape from the chase by USA 270, in March 2022 Shiyan 12-02 executed one or several maneuvers instigating a divergence in its orbit from its partner.

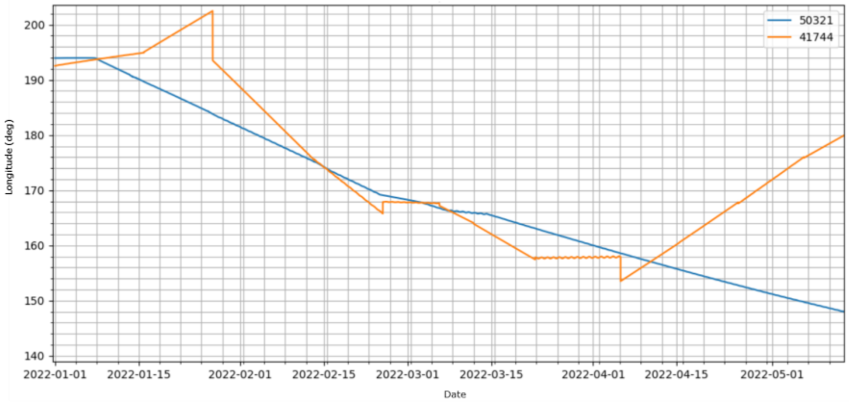

Fig. 2. *USA 270* and *Shiyan 12-01* longitude evolution

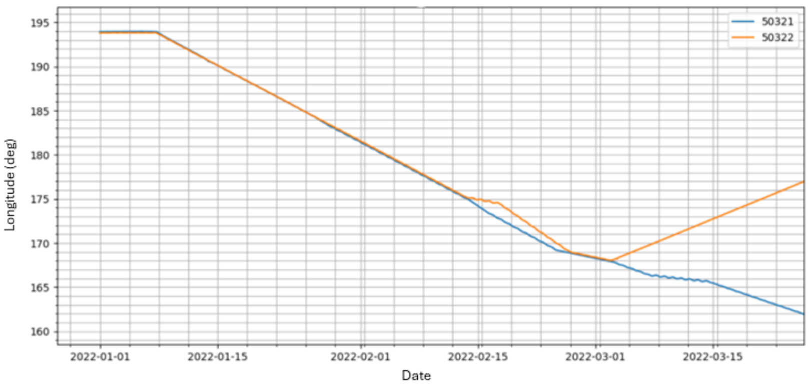

Fig. 3. *Shiyan 12-01* and *Shiyan 12-02* longitude evolution

It is pertinent to highlight that at the inception of the observed period the Chinese satellites appeared to be actively regulatingtheir longitude, maintaining a constant state for approximately seven days. After this period, it is conceivable that they either ceased active control of their longitude, allowing for natural drift, or they adopted a controlled drift that deviated from the prior methodology.

A notable characteristic of these Chinese satellites is their pronounced inclination of approximately 5.3º, which exceeds the customary inclination for satellites in geostationary orbit. This elevated inclination is postulated to be a consequence of experimental operations, as their launch objectives were not aligned with communication functions.

Throughout the observed timeframe, the American satellite *USA 270* undertook an intermittent approach towards these satellites, culminating in several instances of close proximity. As depicted in Fig. 2, *USA 270* pursued *Shiyan 12-01* and *Shiyan 12-02* until early April, maintaining a longitude discrepancy of merely a few degrees. However, after this juncture, *USA 270* maneuvered with the goal of pursuing *Shiyan 12-02*.

In relation to *Shiyan 12-02*, *USA 270* maintained close surveillance until the onset of March. During this interval, *Shiyan 12-02* altered its longitude, which was not mirrored by *USA 270*. Instead, *USA 270* continued its proximity to *Shiyan 12-01* for an additional month. Following this period, *USA 270* executed a maneuver to resume its pursuit of *Shiyan 12-02*, engaging in a gradual but consistent approach. This pursuit persisted for approximately 2-3 months, concluding in July, when *USA 270* started to control its longitude to be near constant until September 2022.

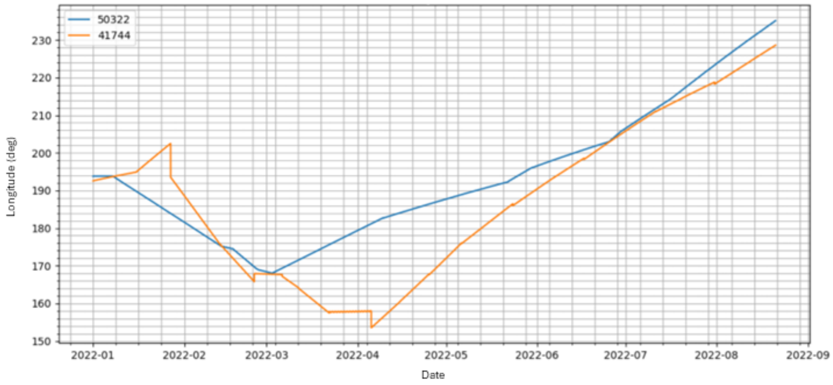

Fig. 4. *Shiyan 12-02* is pursued by *USA 270*

The forthcoming discourse will elaborate on the approaches between the satellites. It is imperative to note that the data pertaining to *USA 270* is somewhat limited, with only 40 TLEs accessible over an eight-month span. While this data suffices to provide a general understanding of the approaches, the precise metrics concerning the closest approach times and distances are estimations.

USA 270 – Shiyan 12-01

It is observed that *USA 270* executed four distinct approaches to this satellite. These proximal encounters occurred on the 8th of January, the 14th of February, the 4th of March, and the 10th of April. During these instances, the duration of proximity was less than one day, a likely consequence of the limited TLE data.

USA 270 – Shiyan 12-02

The approaches between *USA 270* and *Shiyan 12-02* up until March mirror those described previously. The subsequent close approach transpired from the end of June until mid-July. Notably, from March to mid-June, the distance between the satellites was considerably larger due to *USA 270*'s tracking of *Shiyan 12-01* rather than *Shiyan 12-02*. Post-April, *USA 270* gradually altered its longitude until June, when it reached its new target *Shiyan 12-02*. From the 11th of June onward, the satellites commenced a steady drift apart, increasingly distancing themselves from one another.

2.1.3 LEO: KOSMOS-2558 (53323) - USA 326 (51445): 04/08/2022

This case analysis delineates a scenario in LEO, thereby necessitating a distinct analytical approach compared to GEO cases. It involves the Russian satellite *Kosmos-2558* and the American satellite *USA 326*. The latter, being a military satellite, had limited TLEs available, thereby complicating the process of discerning its behavior or identifying its maneuvers.

The satellite *Kosmos-2558* was launched on the 1st of August 2022, and the first close approach occurred on the 4th of August. Upon launch, *Kosmos-2558* was already positioned in an orbital plane closely aligned with its target plane, thereby obviating the need for costly maneuvers.

In order to keep surveillance of the American satellite, *Kosmos-2558* had to match the RAAN variation due to perturbations. Just after its launch, *Kosmos-2558* entered the desired final orbit where it would periodically encounter *USA 326*. The period between close approaches was approximately 5 days and 3 hours, with the minimum distance between the satellites being about 50-70 km and lasted around 10 minutes.

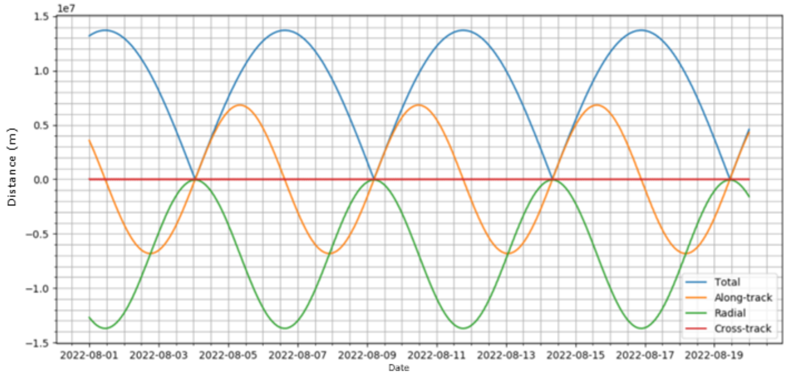

Fig. 5. Distance over time between KOSMOS-2558 and USA 326

In a different manner than GEO malicious CPOs, the operations of the inspector satellite result in a trajectory that is not all the time close to the target satellite. The semi-major axis of *Kosmos-2558* was smaller to generate a drift with respect the inspected satellite to achieve the periodic approach, while ensuring the speed difference was not too large for the approach, allowing the mission to succeed.

2.1.4 LEO: USA 245 (39232) - KOSMOS-2542/2543 (44797/44835): 01/12/19-01/03/20

The case under examination involves two Russian satellites, *Kosmos 2542* and *Kosmos 2543*, which were deployed on an intelligence mission targeting the American satellite *USA 245*. It is important to highlight that *Kosmos 2543* is the result of a Spawning event, where a satellite is deployed from another one.

Kosmos 2542 was launched on November 25, 2019, utilizing the Russian *Soyuz-2-1v Volga* launch vehicle and was placed into a LEO orbit. Subsequently, after a week, *Kosmos 2543* was released from within *Kosmos 2542*, thus being significantly smaller in size.

USA 245, similar to the previous case, is a military satellite, and hence, the total number of Two-Line Element Sets (TLEs) available has been quite limited, which has partially reduced the precision of the results.

Kosmos 2542:

According to the available TLEs, this satellite was directly placed in an orbit that facilitated close approaches with the American satellite at regular intervals. The period of these approaches was approximately 21 days, and the minimum distance reached during these approaches was 46km. This behavior persisted until December 19, 2019.

The orbital plane of both satellites was almost identical, which is a strategy employed by the spy satellite to facilitate espionage tasks. The semi-major axis of the Russian satellite was approximately 17 km lower than that of the American satellite, which enabled it to overtake *USA 245* from behind.

Following this initial stage that concluded on December 19, the American satellite executed a series of maneuvers in which it increased its semi-major axis without altering its orbital plane. The purpose of these manoeuvres is unknown. The *USA 245* increased its Semi-Major Axis (SMA) by about 10 km, which resulted in a decrease in the period between close approaches, from the previous 21 days to 11 days. This scenario lasted until January 21.

The close approaches during this period were as close as 70km on average. During this stage, the orbital planes remained almost identical until the last four days, when *Kosmos 2542* reduced its inclination very slightly by 0.229 degrees, although with no change in RAAN. After this minor change in inclination, *Kosmos 2542* altered its behavior, and instead of performing close approaches at regular intervals, it maintained a very reduced distance from the American satellite from January 22 to February 1. During this period, the distance between the satellites varied daily from 150 to 300km.

Fig. 6 shows the approach and proximity operation performed by the Russian satellite and Fig. 7 depict the relative movement between both satellites during 5 hours in the period where they were in pseudo-constant proximity.

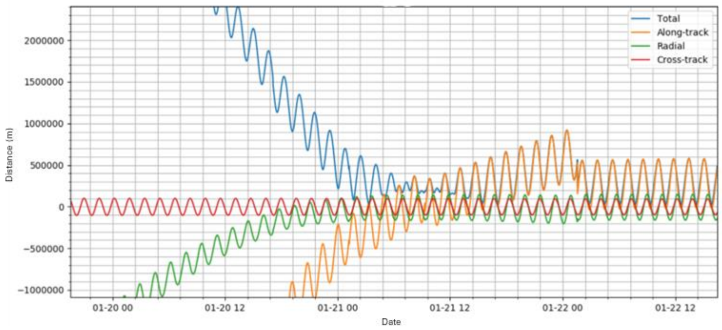

Fig. 6. Approach of Kosmos 2542 to USA

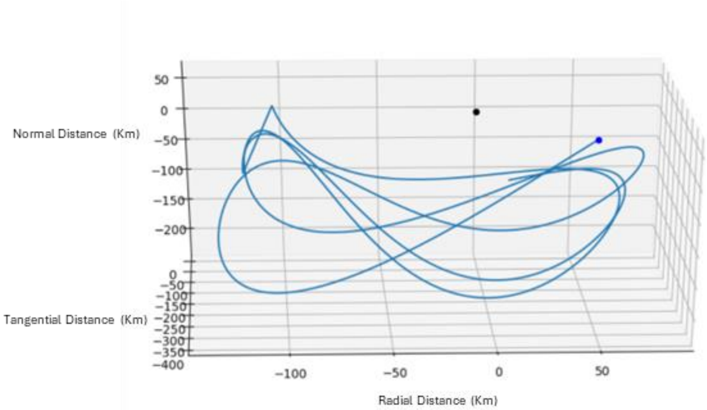

Fig. 7. Relative movement of Kosmos 2542 around USA (km)

During this time both satellites flied in formation with the same semimajor axis. In terms of the orbital plane, both remained almost in the same plane, with a slight difference of 0.23 degrees in inclination and almost the same RAAN.

Finally, after this period, on February 1, both satellites began to slowly increase the distances between each other. This occurred because the Russian satellite slightly increased its SMA, and the difference between both semi-major axes was only 3km. This difference was sufficient to start separating from each other, but with a very long period until they meet again.

Kosmos 2543:

This smaller satellite was detached from *Kosmos 2542* on December 6, 2019, and similarly to the other one, it also performed close approach operations targeting satellite *USA 245*.

The close approaches of these two satellites had two stages. The first one goes from December 6 to December 15, and it can be seen in Figure 8. In this case, the Russian satellite was already in the adequate orbital plane thanks to having been detached from *Kosmos 2542*. The interval of time between every approach was of 12 days, which is almost half the time that *Kosmos 2542* had during this time. Moreover, the closest distance was of about 37.1 km. To achieve it, the difference in the SMA was 14km. During this time, the orbital planes were almost the same with a negligible difference in inclination and RAAN.

After this first stage, the Russian satellite modified its semi-major axis by increasing it by nearly 100km, resulting in larger period than that of the *USA 245*. In such a way, the Russian satellite achieved a sequence of close approaches every 3 days that continued for several months, as it can be seen in Fig. 8. During these approaches, the minimum distance was of between 15 and 25km, which is the closest that the satellites have ever been.

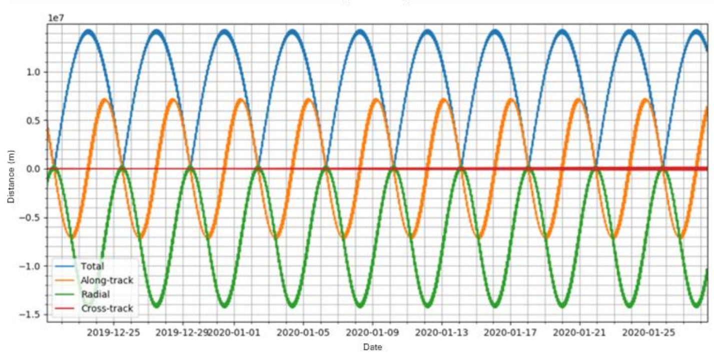

Fig. 8. Distance(m) over time between KOSMOS 2543 and USA 245

2.2 Analysis of Risks associated with neighbours

After the analysis of the different cases above, and the study of how the different inspector satellites behave, there is enough information to proceed with the analysis of the risk posed by neighbour satellites. The cataloguing capabilities provided by SST techniques require a post processing from the point of view of the SDA domain which shall allow to understand the Recognized Space Picture (RSP) and provide the operators of assets of interest with insights about the threats that are posed by other RSOs. There are two scenarios with clear differences in operations regarding malicious CPOs. LEO and GEO. The analysis of real cases has highlighted how these operations are conducted differently in each scenario. Therefore, the analysis of risks has been split in two, to best adapt to each of the scenarios.

Before getting into the analysis of each scenario, it is important to define what are the orbital neighbours. Widely explained, they are the active satellite with orbits close to the monitored asset. Therefore, neighbours not only are in the same orbital regime, but these satellites should also have a similar orbit plane. This statement is inferred from the analysis of real cases. Malicious CPOs are performed with the inspector satellite always in the same orbital plane as their targets in both regimes LEO and GEO. Additionally, the relative velocities of the satellites during the CPOs are always low, which indicates that if the inspector satellite requires big changes in its orbit to reach the target orbit, it is less likely to position itself close enough to carry out its mission in only a few manoeuvres. Encounters with different planes are possible, but speed differences are so big that espionage missions would not be very effective. Additionally, these encounters would occur only once in a very long period.

2.2.1 GEO Regime

In the GEO belt satellites are all collocated in their longitude windows. Moreover, they are relatively in the same plane, with inclination close to zero except for certain cases. On top of that, there are groups of satellites collocated in the same window, flying in formation by positioning differently the equinoctial parameters of eccentricity and inclination.

There are two types of parameters that can be tracked, quantitative and qualitative. The first ones consider the differences between the orbit of the neighbours and the orbit of the monitored asset. For the GEO belt, only the differences in longitude will be considered. Additionally, collocated satellites are not neighbours to be included in the risk analysis, as they are operated by the same organization in almost all cases, or at least, they know they are close to each other and coordinating operations.

The qualitative parameters can be englobed in one scale of how suspicious the neighbour is of being an inspector satellite.

2.2.2 LEO Regime

LEO regime allows for more parameters to be tracked to determine the risk of monitored assets. Within the quantitative parameters, which are the differences between the orbit of the neighbours and the orbit of the monitored asset, it can be used the in-plane and out-of-plane differences. The qualitative parameter is the same one as in GEO, which can be englobed in one scale of how suspicious the neighbour is of being an inspector satellite.

In LEO regime there are much more satellites, and a first filter of neighbours can be induced by the differences in orbital plane, as the plane change manoeuvres too large for almost any mission to consider. They would reduce significantly mission life expectancy. Therefore, only neighbours with very close orbit planes should be taken into account. Getting deeper into this analysis, satellites with similar inclination but different Right Ascension of the Ascending Node (RAAN) and different semi-mayor axis can also be considered, as the secular perturbation on the RAAN would allow it to drift with respect to the target satellite without large out of plane manoeuvres. However, it would not be considered critical, since this drift is not significant enough for the approach to be realised in the short term.

3. RESULTS

Once the proposed methodology has been validated, the resulting analysis of the risk posed by malicious CPOs is presented here, separated in two different scenarios, LEO and GEO regimes. Orbit data is taken from public catalogues, and only TLEs have been used in this analysis.

3.1 Control Volume

In addition to the risk assessment, it is important to note that these encounters usually do not reach distances as small as worrying conjunctions with debris. Regarding RPO event detection, analysed through standard SST conjunction detection techniques, it is very important to highlight differences in the monitored volume around the target satellite. In all cases, as indicated before, approaches are in the same plane using a different semi-mayor axis for drifting towards the target satellite. Therefore, the volume, if defined geometrically in local orbit axes, should be quite long radially, from 50 to 100 km minimum, while 10 kilometres in cross-track and along track should be enough for detecting intentional CPOs in advance.

3.2 GEO Risk Assessment Results

In the first place, we have decided to choose a random monitored asset, the satellite with Norad ID 42741, which from now on will be considered the tentative target of a malicious RPO. Then, we have chosen which are the neighbours to be observed and included in this analysis. In short terms, satellites close to it in the GEO belt. Among these neighbours there is one satellite which is considered of high risk, a proven inspector satellite, and two satellites which are considered as suspicious of having espionage or disruption missions.

After the selection of the asset and the neighbours, there are several manners to provide information on the risk the monitored asset is facing. We have decided to analyse the time it would take for the neighbour satellites to reach their target depending on the delta V used for the relocation to its longitude window shown in Fig. 9.

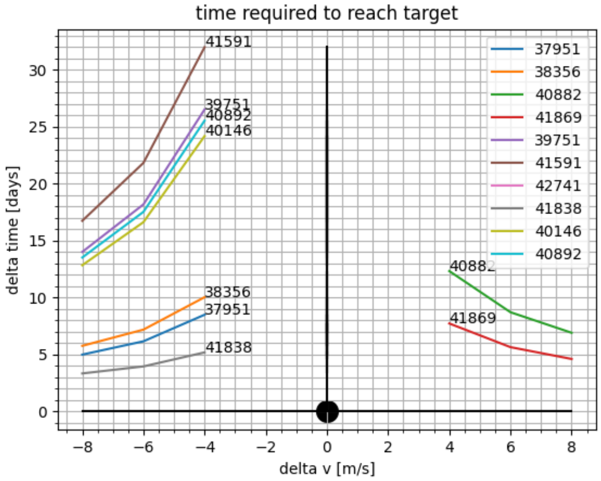

Fig. 9. Time required to reach target by transfer delta V

Previous analysis is based on knowing in advance the possible range of delta V that the inspector satellite is capable of. Additional analysis has been performed according only to the difference in longitude position of the satellites as show in Fig. 10. The following graph shows in each angular position the neighbors of our monitored asset, and the longitude difference included in the radial distance. This allows to visualize directly the danger posed by near active satellites. Moreover, a different mark has been used to differentiate between suspicious neighbors, known inspector satellites and other harmless active satellites.

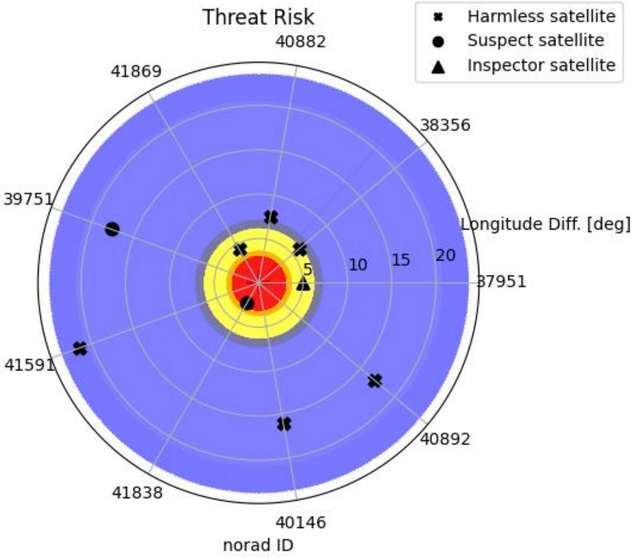

Fig. 10. Risk Assessment for GEO satellite

Closest satellites to our asset could be performing an RPO in less than 6 days by relocating to the same longitude. This time frame is too short to decide on a countermeasure. With this information, operators could be organized in advance to plan for contingencies in case such a threat becomes real.

3.3 LEO Risk Analysis

The risk assessment in LEO regime allows for more quantitative parameters to be included in the analysis. The spectrum of mission orbits is much wider, and it implies further consideration when deciding the neighbours to be included in the risk assessment of intentional RPO. Additionally, in the LEO regime, satellites are more vulnerable as they are easier to reach. Not only by direct ascent ASATs but, as it has been seen in this analysis, objects could be launch directly into orbits with an encounter to an asset.

The monitored asset is the one corresponding to Norad ID 47305, and near satellites with military missions have been selected as his neighbours. For example, the new North Korean satellite, which is known to be an inspector satellite, with Norad ID 58400.

Using the total delta V needed to move to their target's orbit from their current orbit to represent the risk is not useful. When neighbours are not in the same plane, the resulting manoeuvres delta V would be outside the capabilities of any active satellite mission. For that reason, several ways to represent the risk have been found, using the different quantitative and qualitative parameters that can measure the risk of being approached by an inspector satellite. First, showing the normalized value of the parameters considered for each one of the neighbours as shown in Fig. 11. In this case, they are the differences in inclination, RAAN, semi mayor axis, the current delta V to reach the target orbit and if the satellite is considered suspicious.

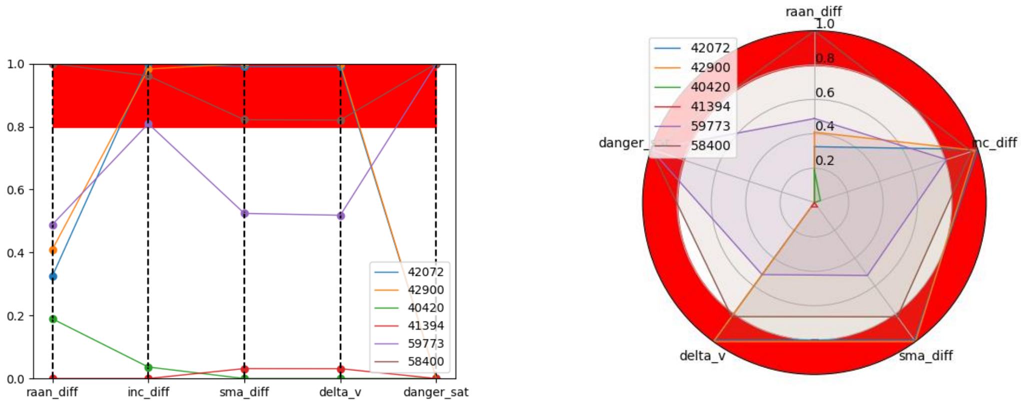

Fig. 11. Risk Assessment in LEO by the normalized value of the parameters

However, neighbours with similar inclination should always be considered because with difference in semi mayor axis, RAAN drift with respect to the target can be achieved. It does not mean that satellites with the same inclination should be considered at higher risk directly, but it will be the most weighted parameter to take into account in the analysis. Therefore, it has been concluded that different weights should be given to each of the parameters used to assess the risk. Thus, a risk level can be computed on a scale from 0 to 100, where 0 represents no risk and 100 represents the highest possible risk (with an inspector satellite in the same orbit as our monitored asset).

Table 1. Weighted parameters

Parameter	Inclination Difference	Semi-mayor Axis Difference	RAAN Difference	Current Delta V to reach target	Know Inspector Satellite (Or Suspicious)
Weight (%)	50	10	10	10	20

Using these weights applied to the different parameters that belong to the Risk Assessment, the following representations of the risk of being a target of a malicious RPO in LEO regime can be found, with the aforementioned monitored asset, shown in Fig. 12. The risk is represented by the risk level from 0 to 100 where 0 represents no risk and 100 indicates an imminent RPO.

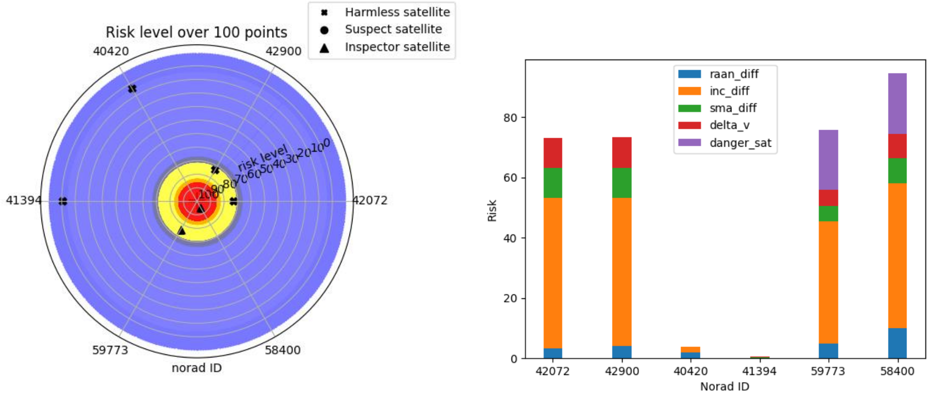

Fig. 12. Radar and Histogram of Risk Assessment

4. CONCLUSIONS

The study of RPOs using a combination of SST and SDA techniques has provided significant insights about how to enhance the monitoring and security of space assets. The integration of SDA and SST capabilities is crucial for the effective monitoring and response to RPOs. This combination allows for the detection, characterization, and mitigation of potential threats posed by inspector satellites. The synergy between these two domains enhances the ability to maintain the security and integrity of space assets.

The study demonstrated the effectiveness of SST techniques in detecting close approaches and potential RPOs. By analyzing the relative positions and trajectories of satellites, it is possible to identify suspicious behaviors and predict potential encounters. This proactive approach is essential for early threat detection and timely response. Characterizing the behavior and capabilities of inspector satellites is crucial for understanding their intentions. This includes analyzing their attitude, pointing behavior, and maneuver patterns to determine whether they pose a threat. The ability to accurately characterize these satellites enhances the overall situational awareness and decision-making process.

The development of risk assessment methodologies allows for the identification of high-risk neighbors and the potential for malicious RPOs. By assessing the orbital differences required for relocation and the qualitative behavior of satellites, operators can plan and execute avoidance maneuvers or other countermeasures. This proactive risk management approach is vital for maintaining the safety and functionality of space assets.

The analysis of real-world cases, such as the interactions between *Luch* and *Intelsat 33e*, *USA 270* and *Shiyan 12*, and *Kosmos-2558* and *USA 326*, provided valuable insights into the behavior of inspector satellites and the effectiveness of detection and mitigation strategies. These case studies highlight the practical applications of the methodologies discussed and underscore the importance of continuous monitoring and analysis.

Continuous improvement of SDA and SST techniques is necessary to keep pace with the evolving space environment. This includes enhancing sensor networks, improving data analysis methodologies, and developing more sophisticated risk assessment tools. Future work should focus on integrating advanced technologies and methodologies to further enhance the capabilities of SDA and SST. Among this work, new AI capabilities could be developed to predict threats with more time in advance, along with a study of a sensors network addressed to SDA goals to study how it can affect the prediction of threats in space.

The operational implications of the findings are significant. Space operators must be equipped with the tools and knowledge to detect, characterize, and respond to RPOs effectively. This requires ongoing training, investment in advanced technologies, and the development of robust operational protocols. The ability to anticipate and mitigate threats is essential for ensuring the long-term sustainability and security of space operations.

The study also highlights the importance of policy and international collaboration in addressing the challenges posed by RPOs. Establishing clear guidelines and fostering cooperation among space-faring nations can enhance the collective ability to monitor and respond to threats. Collaborative efforts can lead to the development of standardized practices and shared resources, further strengthening global space security.

In conclusion, the combination of SDA and SST techniques offers a robust framework for monitoring and mitigating the risks associated with RPOs. By leveraging these capabilities, space operators can enhance the security and sustainability of space assets, ensuring the continued functionality and safety of critical space systems. The findings underscore the need for ongoing research, technological advancements, and international collaboration to address the dynamic challenges of the space environment.

ACKNOWLEDGEMENTS

The authors thank the U.S. Strategic Command for making the catalogue of TLEs publicly available through Space-Track. The authors also thank the Centre for Strategic and International Studies, more specifically the Aerospace Security Project for publishing every year the summary of threats present in the current space scenario, which has allowed to select the most prominent cases of RPOs for this study.

REFERENCES

[1] Clayton Swope, Kari A. Bingen, Makena Young, Madeleine Chang, Stephanie Songer, and Jeremy Tammelleo, *Space Threat Assessment 2024*, the Aerospace Security Project at the Center for Strategic and International Studies (CSIS), 2024 © 2024 by the Center for Strategic and International Studies. All rights reserved.