8th annual Space Traffic Management conference – STM 2022
02-03 March, 2022, Austin, TX, USA

IAA-STM-22-XX-XX

CONSENT TO SHOOT – RETHINKING THE ANTI-SATELLITE WEAPON VERSUS SPACE DEBRIS DILEMMA

Rafal Graczyk[1], **Júlio Mendonça**[1], **and Marcus Völp** [1]

[1]*Interdisciplinary Center for Security, Reliability and Trust, University of Luxembourg,*
6, avenue de la Fonte, L-4364 Esch-sur-Alzette, Luxembourg,
phone: (+352) 46 66 44 - 5984 / - 6315 / - 5634
rafal.graczyk@uni.lu, julio.mendonca@uni.lu, marcus.voelp@uni.lu

Keywords: *space debris, resilience, security, consensus, fault and intrusion tolerance*

ABSTRACT

Space debris, whether caused by anti-satellite weapons or from collisions with defunct vehicles, has become a serious threat to the safe and sustainable use of space. Technologies have been proposed to mitigate this problem by actively removing debris (ADR) by capturing and de-orbiting the targets (e.g., rendezvous operations, tethers, or harpoons) or by indirectly affecting the target's orbit (e.g., using lasers). However, rather sooner than later, deploying ADR technologies against healthy satellites turns the tools for making space safer into anti-satellite weapons, capable of crippling other nations' infrastructure. In an attempt to resolve the tool-versus-weapon dilemma, we discuss in this paper technical solutions that involve a paradigm shift in the Concept of Operations, but that also have the potential to avoid political implications and many concerns that currently prevent us from solving the space-debris problem. The solutions we advocate require consensus between involved stakeholders for all critical operations of an ADR system. We show it is technologically possible and, in fact, already well understood how to enforce that such operations can only be performed consensually. We sketch a distributed infrastructure, capable of supporting such operations among all stakeholders, enforcing agreement in international cooperation about where and for how long an ADR system gets activated, what targets it follows and where safety zones and objects are. In this way, stakeholders have to validate every piece of information to remove single points of failures, but more importantly to put the required mutual trust on solid and technologically enforced foundations.

1. Introduction

Over the past decade, the amount of vehicles humanity has deployed in space has grown almost exponentially, resulting in more than 4400 active vehicles in the near-Earth space maintained today [1]. At the same time, the amount of space debris has reached a level where safe and sustainable operation in certain orbits has already exceeded the natural debris deorbiting rate and hence the environment's self-cleaning capabilities, by several orders of magnitude, creating severe threats. For example, from the perspective of active objects operators, information about other objects is very limited, incomplete and is bound to quickly get outdated. Agreeing on maneuvers to evade existing debris (or other payloads) is therefore, in many cases, burdensome, if possible at all [2] and, in any case, negatively affects the lifetime of space vehicles. Several researchers and practitioners even believe that without active measures, Kessler's syndrome [3] (i.e., a self-reinforcing avalanche effect of debris hitting other satellites, creating more debris, etc.) can no longer be avoided.

Of course, we know by now several methods how to actively free near-earth space from still active vehicles [4] and thereby reduce the risk of increasing this form of pollution in the future. We also know about several measures to capture and deorbit defunct and passivated vehicles [5] and first demonstrator missions for such technology has be launched [6]. However, despite our crucial dependence on near Earth space, we are also facing the general fear of a dual use of this technology, namely to attack and actively destroy or damage an opponent's satellites, whether for commercial profit, as part of military engagements, or simply as an act of terrorism (e.g., after compromising the software of anti-debris platforms). This fear is particularly present for technologies such as Laser-based Orbital Debris Removal (LODR) platforms, that can be used multiple times to free orbits from more difficult to track, smaller debris, but equally well to damage larger and still functioning satellites. In particular, if such platforms fall in the hands of terrorists, existing strategies, including the threat of considering an attack in space equal to a territorial breach on ground, turn into futile attempts. And when we consider that the location of origin of cyber-incidents of this sort needs not necessarily match the location of the affected equipment (attack attribution ambiguity), physical retribution turns into an empty threat, or worse into one that if at all hits the wrong actors.

In our opinion, it is this dual use of anti-debris technology as anti-satellite weapons that prevents large scale efforts to globally address the space debris problem, while we still have the chance to solving it. Therefore, in this paper, we highlight specifically on the example of pusher laser facilities (but easily transferable to other debris removal technologies), which technical solutions already exist to secure debris removal while, at the same time, avoiding misuse of the same technology to attack still functioning satellites. In particular, we shall see that from a technical perspective nothing speaks against an international effort towards deploying mutually controlled anti-debris technology to help clean space, even if on other matters the involved parties disagree.

After introducing the necessary background on today's state of space situational awareness (SSA) and the active debris removal (ADR) techniques that have been proposed, we shall focus on consensus technologies as a guiding principle, both during operation and at several technical levels, gives rise to secure debris removal on Section 2. We introduce in Section 3 an example control system architecture for preventing the misuse of such technology as anti-satellite weapon, discuss operational concepts and technical solutions, before we wrap up in Section 4 by drawing our conclusions about the potential implications of such technological aspects.

2. Background

2.1 Space Situation Awareness (SSA)

According to NASA, SSA comprehends "the current and predictive knowledge of the space environment and the operational environment upon which space operations depend" [7]. The European Space Agency defines it as a set of capabilities for providing timely and accurate information regarding the space environment, particularly hazards to infrastructure in orbit and on the ground [8]. Nowadays, the USA's Space Situational Awareness has more capabilities than any other SSA systems [7]. The U.S. Space Surveillance Network (SSN) tracks more than 23,000 objects composed of active satellites, defunct satellites, and pieces of debris, providing the vastest identification and tracking information of objects in orbit [8]. This track information is used as a resource to avoid damaging collisions between satellites and other space objects. Therefore, developing and disseminating this data is crucial for planning safer space operations. However, in the event of losing this data (e.g., in the course of a malicious incident), space operations of entire nations may be compromised. Note that this information is sensitive, and it is unlikely that other nations will share critical or complete data. Using this data, one could detect, track, interfere, or destroy a satellite, for example [9]. Although public services and databases (e.g., Space-Track[1]) offer some information, they are known to be incomplete or insufficient to enable space operations. Hence, only tracking and sharing data regarding space objects may not be sufficient, representing, in an operation-view, a single point of failure. Enabling other ways to create safe and trusting mechanisms to avoid collisions with space debris is crucial for advancing space operations. Therefore, next, we describe ADR technologies and consensus technologies that might be the key to enabling large-scale ADR methods.

2.2 Debris Removal Techniques

Active debris removal involves pulling obsolete spacecraft (satellites and rockets) or fragments of spacecraft that have broken off satellites and rockets through an external disposal method (e.g., safely de-orbiting or destruction) [10]. Mark and Kamath [5] conducted a survey and pointed out eight different classifications for ADR techniques: (1) Laser-based, (2) Tether-based, (3) Satellite-based, (4) Dynamical Systems-based, (5)

[1] https://www.space-track.org

Collective, (6) Ion beam shepherd-based, (7) Sail based, and (8) Unconventional. Although all of these techniques need further investigation, according to the authors, the tether-based and dynamical systems-based methods are leading the research development. The tether-based concept involves connecting a long wire to a piece of debris and letting the Earth's magnetic field act on it to slowly pull the vehicle back into the atmosphere. Dynamical systems-based ADR methods involve de-orbiting the debris by altering the orbital parameters through a combination of natural and artificial perturbations. However, both tether-based and dynamical systems-based techniques seem unsuitable for large-scale removal, and their action may take too long. On the other hand, laser-based techniques have been proved suitable for mass-scale debris removal while presenting relatively low implementation costs [11], since the platform can be reused multiple times. In this technique, a high-frequency pulsed laser beam is shot into space debris to vaporize it's surface and, by creation of ablation jets, alter its velocity vector to decrease its perigee and increase the experienced residual atmospheric drag. As a result the targeted space debris would deorbit significantly quicker, than in, do-nothing case. According to Phillips et al. [11], the technique can be feasibly operated from both ground or from space and has been proven to as well effectively remove debris of irregular shapes [12].

Although technically feasible as an ADR method, some issues emerge regarding weaponizing space. In fact, several analysts believe Reagan's SDI-programme would have brought us to the brink of a nuclear war had high-power lasers been available at the time [13]. Now they are and the possibility of one having high-power lasers capable of destroying debris can raise concerns of third parties regarding their space assets not being attacked. The DE-STAR concept [14] presented a high-power laser-based weapon to be located on the moon capable of vaporizing rocks over one Astronomical Unit (AU) away. In the wrong hands, this kind of system could be used against targets on Earth. Kaushal and Kaddoum [15] discussed several laser technologies that have the potential to be used as weapons and damage long-distance targets from both ground and space. Lastly, the Russian Sokol-Eshelon project is a well-known example of how laser-based technology can be used as an anti-satellite weapon. In 2009, the Sokol-Eshelon successfully executed a test to illuminate the Japanese satellite AJISAI at an orbital height of 1,500 km and picked up the reflection of the laser [16].

2.3 Consensus technologies

One of the main arguments in this paper is our claim that technologies for securing space debris removal are already in place, although they require rethinking how systems are constructed and operated. Let us therefore also introduce some of these technologies, namely to enforce agreement or consensus on the critical operations to perform. Consensus technologies enable a system to reach an agreement on operations or data values even though some system processes are faulty (e.g., misfunction or malicious behavior) [17]. These technologies are mainly applied for distributed systems to ensure fault tolerance and resilience, even if system processes communicate over an unreliable network. Developed solutions employing consensus technologies are usually addressed as Byzantine-fault tolerant (BFT) systems since the system can work properly even in the presence of a Byzantine fault (when components operate arbitrarily) [18]. Practical usages in large-scale systems such as clouds [19] and blockchains [20] and critical systems such as aircraft controls [21, 22] have demonstrated the effectiveness of consensus technologies and shown that they are already well established for enforcing consensual operations and providing fault and intrusion tolerance capabilities [23]. For the purpose of this paper, we will extend the scope of fault to entities and interest groups that aim at jeopardizing missions, whether by unilaterally trying to misuse the vehicle's capability or by attacking its software to follow their command. Our goal is to tolerate such single-handed malicious actions, masking them behind an overruling majority of the remaining stakeholders, operating in consensus for the purpose of clearing space without causing damage.

Some works have already been proposed to increase the resilience of SSA systems using consensus technology. For example, Jia et al. [24, 25] proposed a consensus-based distributed sensor management algorithm for space object tracking. The algorithm is used to select tracking tasks and achieve agreements between the data collected by different sensors. Similarly, Wei and Nener [26] presented a consensus algorithm for space debris tracking. The proposed algorithm could be used in distributed space debris tracking systems. It adopted iterative consensus among neighboring nodes of the system to achieve consensus of tracked objects. Other works have proposed developing a distributed (and blockchain-based) infrastructure for SSA data acquisition and distribution (e.g., using the Hyperledger framework [27]) where no single entity is responsible for holding and processing the SSA data. Xu et al. [28] proposed to combine ground SSA distribution systems with space segment maneuver control in one blockchain-based system. Reed et al. [29] proposed a distributed blockchain as an alternative to the single owner/operator information-sharing model of SSA data. In our earlier work [30], we proposed a distributed and blockchain-based ephemerides storage and distribution system, aiming at maintaining safety and security guarantees in the presence of active attackers or severe faults. However, no work has considered using consensus technologies as a game-changing enabler for ADR systems. Therefore, in the following sections of this paper, we discuss a solution that has its foundations on consensus technologies to enforce an agreement between different stakeholders for using large-scale ADR systems in a trusted manner.

3. Laser-based Orbital Debris Removal Control System Architecture

In the following, we describe a multi-stakeholder system, deployed internationally among a federation of legitimate space-faring organizations that aim towards the common goal of tackling the space debris problem at scale. By legitimate, we mean any space faring nation, focusing primarily on a civil use of space, but not terrorist organizations. Such nations will share the common view that space debris orbiting Low Earth Orbit threatens to jeopardize every nations' capability to utilize space. In other words, we start from a "coalition of the willing" where participating members are ready and willing to build and operate a system of ground-based laser stations and, possibly as the next step, space-borne laser platforms to remove debris. We do not require trust among these members and will in fact allow for certain activities, such as space-based espionage, which by its nature needs to be hidden from the others and may cause disapproval when detected. Nevertheless, such a characterization of members supports space-debris removal, provided the means for that are operated in a safe manner. We show, that safety in such a system can be achieved by distributing the physical elements of the system and by logically centralizing the decision making and information distribution. We assume that members of this "coalition of the willing", even among themselves, might be reluctant to share classified SSA data (e.g., the location of spy satellites), as well as, to disclose accuracy, precision and coverage of their SSA capabilities. The latter might be deemed matters of national security. Our solution therefore opts for a "veto" mechanism, to be deployed when an own spy satellite crosses the region of debris removal, by allowing each member to halt the system operation. Debris removal should be halted in case of potential detection faults, but also, when there is a risk that the laser operation might, unintentionally, affect the operation of classified systems and, to not disclose their presence, also occasionally if they are not there. Vetoing does not require a nation to disclose a particular reason for exercising this mechanism, but of course a nation should not veto all operations as this would defy their intention to remove space debris.

Our system consists of three parts:

- a cloud-based database which contains agreed upon (among the participants of the federation) ephemeris of objects that should be pushed by the laser;
- the second part are ground or in-orbit based observation stations. This second part of the system provides the technical means for cross-checking which object shall be affected and by which ground or in-orbit based laser and when;
- the ground or in-orbit based laser that is used to push debris out of orbit and into the atmosphere.

Our goal is to prevent any stakeholder and externals from utilizing the latter without first reaching agreement with the others. We therefore ensure that a consensual decision is transferred to a laser stations by all parties and that the laser station itself is equipped with a plurality of safety modules, each of the belonging to one of the members to prevent misuse of the platform by the others. Security modules are the remote control outposts of involved nations and control the activation of the laser and similar critical operations. In contrast, no nation is in control of the consensus mechanism itself, which we propose to develop as an open source mechanism to ensure analysis by each member and which will be deployed if all nations clear this component. Control outputs ensure control and safety of the laser infrastructure.

As already indicated, the crux behind the tool versus weapon dilemma, in case of LODR, lies in the fact that the pusher laser system can be used with either good or malicious intentions. LODR can be deployed against defunct systems or debris following the intention to create ablation jets or plasma and, over time, to alter their orbits in such a way that they deorbit themselves quicker. The same technique deployed against operating payloads will be destructive to their optics (observation payloads, sun sensors, horizon detectors, star trackers), solar arrays (thermal-mechanical or semiconductor damage, open circuits due to metal connections vaporization) or propulsion (piercing the tanks and loss of pressurized propellant resulting in uncontrolled spin). Targeting and affecting operational payload must therefore be avoided at all cost. This goal lies at the heart of the system Concept of Operations and Technical implementation, on which we will elaborate in the following sections.

3.1 Concept of Operations

In order to ensure system safety of operation without the need to disclose confidential data and without the need to fully establish trust between participants, we propose to run the distributed consensus among the system participants in the following manner:

- members reach agreement on the objects to be removed (debris, defunct or passivated payloads) database;
- the agree on the contents of the active non-confidential payloads database;
- and they give their consent to the positioning of the pusher laser facility (especially if mobile).

Mentioned datasets are sufficient to propose the cleaning zones where laser-based ADR activities will be confined to space and time agreed by the stakeholders. The latter will help the operators of confidential payloads to possibly avoid, by outmaneuvering, the cleaning zones. Stakeholders which suspect they will not be able to maneuver out of the cleaning zone will have to "veto" the removal. This may seem radical but, first, we are in a situation where humanity needs to clean space to continue to use space. Permanent vetoing will not help alleviate the current situations and stakeholders will need to agree to ensure any improvement, most of the times when none of their secret vehicles are in danger. Second, the "veto" mechanism may have hidden penalties of disclosing some of the information on the classified object since other parties could try to reverse engineer possible trajectories from the vetoed cleaning zones, their time and location in space. This however can be gamed by issuing unnecessary "vetos" from time to time, adding noise to the system and to the attempt to reconstruct hidden vehicle trajectories. Other forms of penalties could include social and or political pressure to agree in principle to debris removal.

The described management, control and data distribution system is compatible with, both, ground and space-borne Laser-based Orbital Debris Removal (LODR) activities.

Ground based LODR stations, most likely, will be distributed on the equator and in polar regions. It can be assumed that those station are not mobile, but there may also be mobile variants (e.g., deployed on aircraft or, more likely, maritime vessels). The cleaning field of such a unit is static relative to its location and the laser's field of view (FoV). It will also have an effective depth of operation, perhaps few hundred kilometers, realistically up to 1000 km, depending on the laser's power and its mirror aperture. An essential requirement for our solution to work is that despite the laser being possibly located in a country, physical access to its firing capabilities must be prevented at all costs, up to the extent of destroying the laser, should the owning nation attempt to use it unilaterally.

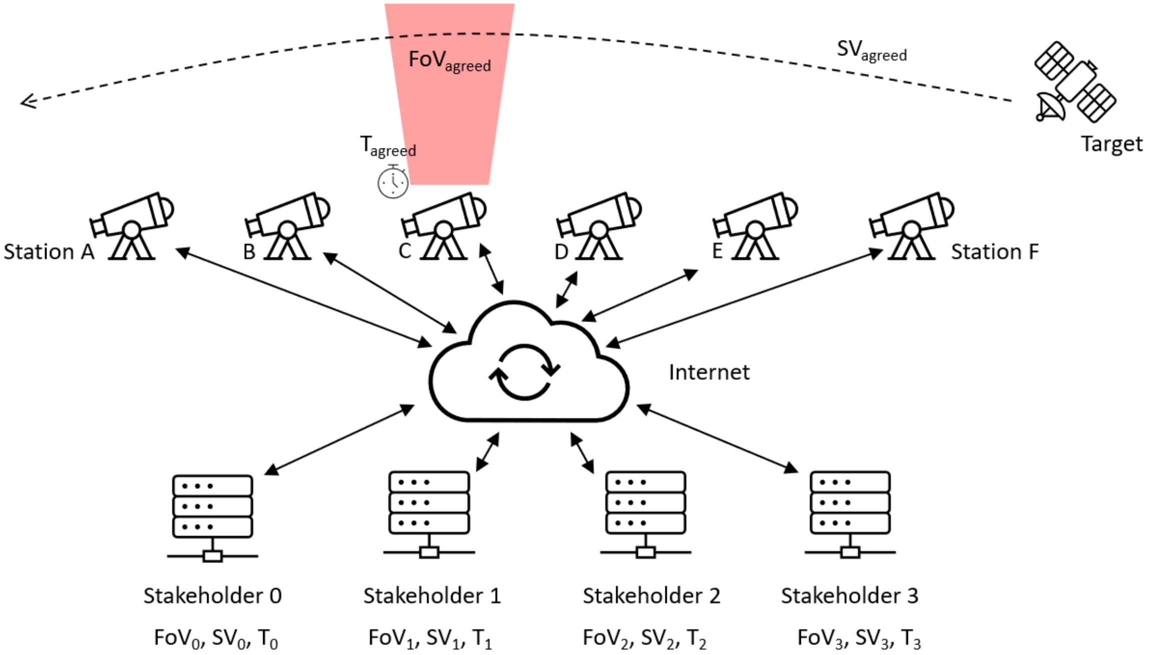

Figure 1. Concept of Operations.

Space-based LODR satellites could be placed in various orbits, with SSO dusk-dawn being an obvious bet due to congestion and power generation consideration. Space based laser sweepers can be effective only against co-orbital objects. It is therefore safe to assume that cleaning fields are behind and ahead of the sweeper. In all other orbital configurations the rate at which objects enter and leave the laser's FOV will most likely be too quick for an effective operation.

In our Concept of Operations (Fig. 1), we therefore assume that there are a few, mutually independent stake holders, interested in employing a LODR for cleaning up near Earth space. Our goal is to achieve the desirable property of Byzantine Fault Tolerance (BFT, refer to Section 2.3) and ensure that up to f faults or intrusions will have no negative effect. To ensure this, there shall be $3f + 1$ mutually independent stakeholders. In the process of implementing BFT and ensuring that the system becomes at least free of single points of failure (or malicious deterioration), that decision on laser station current time, position and pointing as well as the contents of the ephemeris ledgers for all objects to be laser swiped, should be made consensually. That is, all members should collectively agree on this decision by running an exact or approximate, depending on context, agreement algorithm on data sets provided by the involved stakeholders. For that, each stakeholder leverages its enforcement node to case a vote for distributed control and the infrastructure ensures that all decisions that are taken within the system are taken by a safe majority.

Anticipating both accidental and malicious compromise of some of the stakeholder's control components, this majority can be a life and safe quorum Q:

$$\begin{aligned} \textit{life}: &\quad |Q| \leq n - f && (1) \\ \textit{safe}: &\quad [2Q] - n \geq f + 1 && (2) \end{aligned}$$

which of course assumes that all stakeholders in general apply technically correct solutions that, aside from cyberattacks, remain under their control. On the contrary, for making the decision to shoot in the first place, lifeness must be sacrificed quorums with $|Q| = n$ must be chosen.

Each of the stakeholders shall be capable of providing, to the laser stations, its own time distribution and position services (GNSS), shall be capable of space objects detection, ephemeris estimation (all active, passive, debris, own confidential) and propagation the trajectories with accuracy sufficient for pusher laser to acquire target and progress into active target tracking. Stakeholders shall be also capable of deploying hardware and software for communication with and processing at the laser stations. The time and position service is required to keep the stations synchronized and localized if they are mobile. This is used for establishing each station's field of view and for predicting when objects or subjects of cleaning will enter and leave the station's FOV, effectively establishing the time of laser operation.

3.2 Technical Solution

Figure 2 describes in greater detail the exact solution we propose for controlling the Laser-based Orbital Debris Removal (LODR) station.

Safety Modules. There shall be a Safety Module (SM) designed (according to a common specification of interfaces and operations), manufactured, assembled, integrated on site and tested by each of the stakeholders. These SMs shall act like remote outpost, at the protected facility of the pusher laser, providing the stakeholder with telecommand and telemetry capabilities. Telecommands means that stakeholders shall be able to provide the schedule of debris removal operations, indicating the expected target trajectory, pointing coordinates and time of target acquisition computed and collectively agreed in the CONOPS cloud, providing key functionality for defining laser operations. Telemetry means that, independently of others, the SMs shall be able to report back on, actuation inputs provided by others, the state of the pointing, position of the facility, local time and state of the synchronization. Notice, that this does not necessitate a separate communication link. A virtual channel, cryptographically protected, suffices to convey such commands, since failure of communication can always be mapped to exercising the "veto".

Each SM separately shall provide localization functionality utilizing signals from several independent ($n = 3f + 1$ for up to f failures or attacks; e.g., $n = 4$ for $f = 1$) global navigation satellite systems (GNSS). For mobile stations, an inertial measurement unit could be considered, but a power-accuracy trade-off shall be conducted. It is allowed that safety modules receive more than one GNSS network, as long as internally, the resulting final position is established.

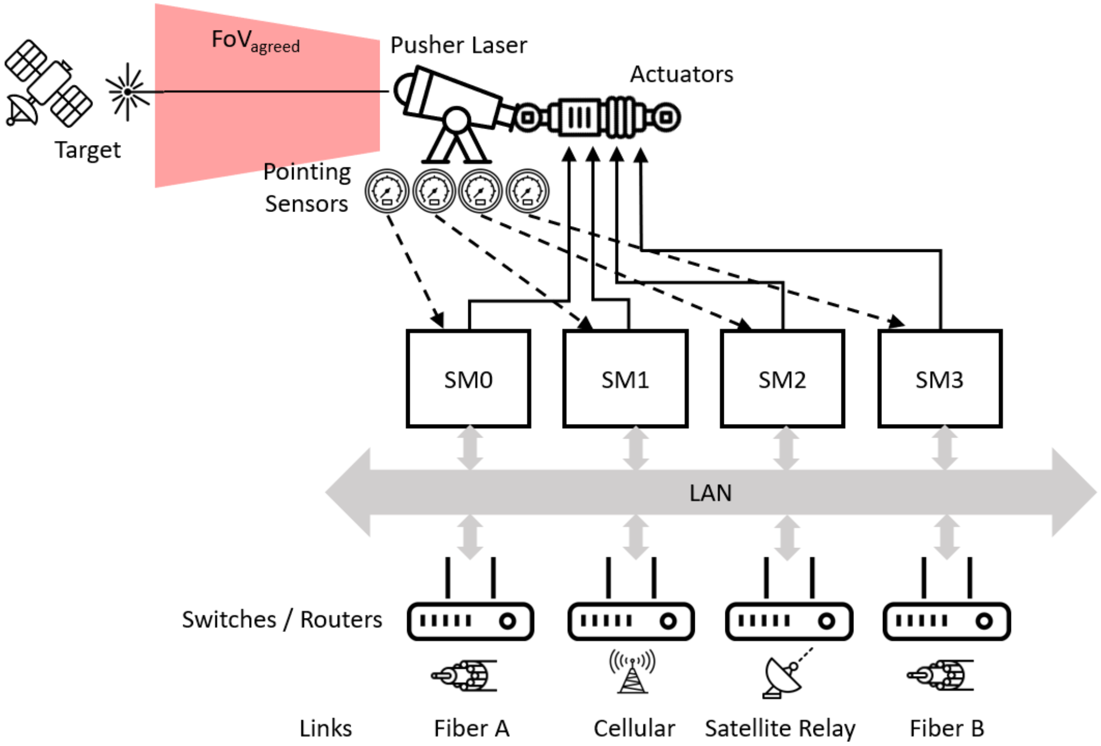

Figure 2. Technical solution for controlling the LODR station.

Local control. Within each station mirrors for laser pointing are actuated by set of actuators. Actuators have to be consensually driven by SM. Meaning that each of the actuators is smart, it has capability to collect the suggestions proposed by the SM's and act according to what is proposed by majority of SM's. At the same time effects of the actuation are continuously monitored by all each and every SM.

The pusher laser control has to be to some extent autonomous. When the object of interest enters the laser facility FOV, based on its agreed ephemeris, the passive acquisition starts – object has to be flashed by burst of low-power laser light. The reflected and received signal confirms the correctness of space object ephemeris and laser system actuation. The sensor readout shall be fed back to all the SM's for confirmation of expected system operation. At this stage, control shall be (consensually, by majority of SM) handed over to autonomous active tracking system, which turns on high pusher laser power and, thanks to adaptive optics, starts focusing the beam on the object, initiating the LODR process. After the target got acquired it will be followed autonomously and SMs need to check what is going on and at any sign of increased risk or ambiguities in correctness of tracking the laser operation shall be vetoed. While active control of the pusher laser beam might also be distributed among the SM's, it is not required, since it adds unnecessary complexity and timing requirements. To ensure safety of the system operation it shall be sufficient, for all the SM's, to monitor the LODR process, and veto the laser operation as soon as soon as the tracking is lost – for this purpose chain of laser-power kill switches is constructed as shown on Figure 3. Effectively, for laser station to operate, all of the kill-switches must be enabled.

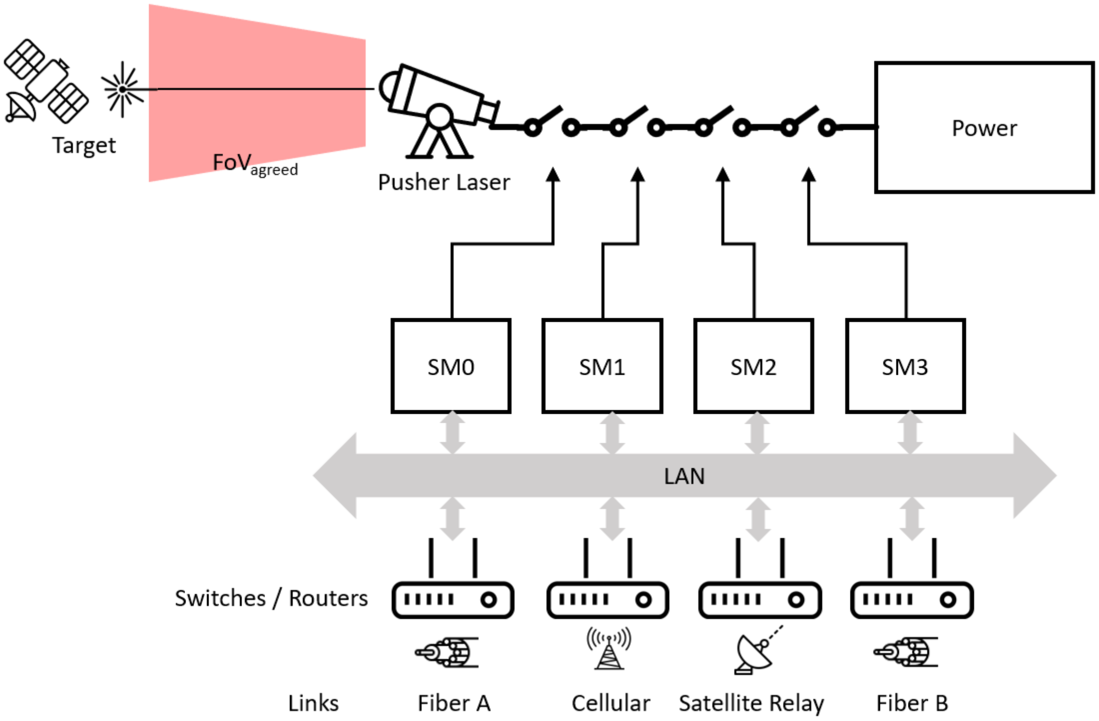

Figure 3. Technical solution for veto mechanism in LODR stations.

Connectivity. Each of the stake holder shall provide own and independent of others means of communication with the facility. The more diverse ways of implementation, the better. Communication means under consideration – fiber, GSM networks, commercial satellite broadband via VSATs, satellite relays (multi-hop possible). The communication links are fed to routers which also provide internal IP network switching capabilities, so data packets can actually be fed through any of the links, regardless of operating stakeholder. This is also the reason for logical separation of the networks, deployed on shared physical networking medium, by establishing VLANs.

Power. Depending on the laser system debris removal variant – stationary or mobile, the power shall either be provided from the grid or from the off-grid sources (Photovoltaic (PV) farm, fuel cells, or internal combustion generators). Also, depending on particular circumstances and feasibility of implementation, a secondary or back-up power sources might be added to increase the availability of the facility.

4. Conclusions

In this paper, we have introduced a distributed multi-stakeholder concept for securing laser-based orbital debris removing (LODR) infrastructure against misuse by individual stakeholders, whether they are members of the infrastructure consortium or outside actors, aiming at ceasing control through cyberattacks. Our goal was to provide technical solutions for information exchange and consensus-based control mechanisms that are capable of withstanding faults, whether accidental or intentionally malicious (e.g., resulting from security breaches). We achieve that on the implementation/technical side through extensive hardware and software diversification and through communication-link hybridization. On the concept of operations side, we enforce consensus through a built-in, incircumventable agreement capability, allowing any legitimate stakeholder to veto operating the laser, while discussing the consequences of constant veto. That is, even though a single legitimate partner may constantly veto space-debris removal, we would not worsen the situation, but just return to the situation we have now, where nothing is done to remove space debris, leaving it to the political floor to convince stakeholders that at least occasionally it is in the interest of human mankind to actually use these new capabilities. Our solution is applicable to space-based LODR and equally to ground-based, provided physical access to the laser is prevented through other means. Moreover, presented consensus mechanism can be extended and used for ensuing collective control over any type of space debris cleaning infrastructure, especially when it can, accidentally or maliciously, get weaponized. In the future, we plan to investigate similar technologies for securing semi-automated lunar regolith harvesting and in-situ resource utilization, both of asteroids and by scavenging satellites in the GEO graveyard.

REFERENCES

[1] ESA Space Debris Office, "Esa's annual space environment report," 2021. [Online]. Available: https://www.sdo.esoc.esa.int/environment_report/ Space_Environment_Report_latest.pdf

[2] M. Wall, "European Satellite Dodges Potential Collision with SpaceX Starlink Craft," 2019, [Online]. https://www.space.com/ spacex-starlink-esa-satellite-collision-avoidance.html. Accessed on 10/02/2022.

[3] D. J. Kessler and B. G. Cour-Palais, "Collision frequency of artificial satellites: The creation of a debris belt," Journal of Geophysical Research: Space Physics, vol. 83, no. A6, pp. 2637-2646, 1978.

[4] European Space Policy Institute (ESPI), "Towards a european approach to space traffic management," 2020. [Online]. Available: https://espi.or.at/publications/espi-public-reports/send/ 2-public-espi-reports/494-espi-report-71-stm

[5] C. P. Mark and S. Kamath, "Review of active space debris removal methods," Space Policy, vol. 47, pp. 194-206, 2 2019.

[6] Astroscale, "Astroscale Statement on Our ELSA-d Demonstration," 2022, [Online]. https://astroscale.com/ astroscale-statement-on-our-elsa-d-demonstration/. Accessed on 12/02/2022.

[7] B. Lal, A. Balakrishnan, B. M. Caldwell, R. S. Buenconsejo, and S. A. Carioscia, "Global trends in space situational awareness (SSA) and space traffic management (STM)," INSTITUTE FOR DEFENSE ANALYSES WASHINGTON DC, Tech. Rep., 2018.

[8] Space Security Index, "Ssi issue guide - space situational awareness," Space Security Index, Tech. Rep., 9 2020.

[9] B. D. Green, "Space situational awareness data sharing: safety tool or security threat?" The Air Force law review, vol. 75, p. 39, 2016.

[10] C. R. May, "Triggers and effects of an active debris removal market," The Aerospace Corporation, Center for Space Policy and Strategy, Tech. Rep., Jan 2021. [Online]. Available: https://aerospace.org/sites/default/files/2021-01/adr%20paper.pdf

[11] C. R. Phipps, "A laser-optical system to re-enter or lower Low Earth Orbit space debris," Acta Astronautica, vol. 93, pp. 418-429, 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0094576513002749

[12] S. Scharring, J. Wilken, and H.-A. Eckel, "Laser-based removal of irregularly shaped space debris," Optical Engineering, vol. 56, no. 1, p. 011007, 2016.

[13] U.S. Department of State, "Strategic Defense Initiative (SDI), 1983," 2022, [Online]. https://2001-2009.state.gov/r/pa/ho/time/rd/104253.htm. Accessed on 02/02/2022.

[14] G. B. Hughes, P. Lubin, J. Bible, J. Bublitz, J. Arriola, C. Motta, J. Suen, I. Johansson, J. Riley, N. Sarvian et al , "De-star: phased-array laser technology for planetary defense and other scientific purposes," in Nanophotonics and Macrophotonics for Space Environments VII, vol. 8876. SPIE, 2013, pp. 132-146.

[15] H. Kaushal and G. Kaddoum, "Applications of lasers for tactical military operations," IEEE Access, vol. 5, pp. 20 736-20 753, 2017.

[16] Russian strategic nuclear forces, "Russia has been testing laser ASAT," 2011, [Online]. https://russianforces.org/blog/2011/10/russia_has_been_ testing_laser.shtml. Accessed on 10/02/2022.

[17] G. Bracha and S. Toueg, "Resilient consensus protocols," in Proceedings of the second annual ACM symposium on Principles of distributed computing, 1983, pp. 12-26.

[18] Y. Xiao, N. Zhang, J. Li, W. Lou, and Y. T. Hou, "Distributed consensus protocols and algorithms," Blockchain for istributed Systems Security, vol. 25, p. 40, 2019.

[19] M. N. Cheraghlou, A. Khadem-Zadeh, and M. Haghparast, "A survey of fault tolerance architecture in cloud computing," Journal of Network and Computer Applications, vol. 61, pp. 81-92, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804515002246

[20] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), 2017, pp.1-5.

[21] J. Rushby, "Bus architectures for safety-critical embedded systems," in International Workshop on Embedded Software. Springer, 2001, pp. 306-323.

[22] Y. Yeh, "Safety critical avionics for the 777 primary flight controls system," in 20th ASC 20th igital Avionics Systems Conference (Cat No 01CH37219), vol. 1, 2001, pp. 1C2/1-1C2/11 vol.1.

[23] G. S. Veronese, M. Correia, A. N. Bessani, L. C. Lung, and P. Verissimo, "Efficient byzantine fault-tolerance," IEEE Transactions on Computers, vol. 62, no. 1, pp. 16-30, 2011.

[24] B. Jia, K. D. Pham, E. Blasch, D. Shen, Z. Wang, and G. Chen, "Cooperative space object tracking using consensus-based filters," in 17th International Conference on Information Fusion (FUSION). IEEE, 2014, pp. 1-8.

[25] B. Jia, K. D. Pham, E. Blasch, D. Shen, and G. Chen, "Consensus-based auction algorithm for distributed sensor management in space object tracking," in 2017 IEEE Aerospace Conference. IEEE, 2017, pp. 1-8.

[26] B. Wei and B. Nener, "Distributed space debris tracking with consensus labeled random finite set filtering," Sensors, vol. 18, no. 9, p. 3005, 2018.

[27] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich et al , "Hyperledger fabric: a distributed operating system for permissioned blockchains," in Proceedings of the thirteenth EuroSys conference, 2018, pp. 1-15.

[28] R. Xu, Y. Chen, E. Blasch, and G. Chen, "Exploration of blockchain-enabled decentralized capability-based access control strategy for space situation awareness," Optical Engineering, vol. 58, no. 4, p. 041609, 2019.

[29] H. Reed, N. D. Dailey, R. Carden, and D. Bryson, "Blockchain enabled space traffic awareness (besta): Discovery of anomalous behavior supporting automated space traffic management," in ASCEN 2020, 2020, p. 4105.

[30] R. Graczyk and M. Voelp, "Ephemerishield - defence against cyber- antisatellite weapons." NATO Science & Technology Organization, Applied Vehicle Technology Panel, 2021. [Online]. Available: http://hdl.handle.net/10993/49361