An Analysis of the Potential Misuse of Active Debris Removal, On-Orbit Servicing, and Rendezvous & Proximity Operations Technologies

James Alver

Andrew Garza

Christopher May

Prof. Kei Koizumi, Elliot School of International Affairs

The George Washington University

06 May 2019

Completed as part of the capstone requirement for the conferral of Master of Arts, Int'l Science and Technology Policy (Space Policy), and on behalf of the capstone client, Secure World Foundation.

Executive Summary

Systems that are capable of more autonomous Rendezvous and Proximity Operations (RPO), in particular On-Orbit Servicing (OOS) and Active Debris Removal (ADR) systems, are on the verge of becoming commonplace in the coming decade. Both ADR and OOS use Rendezvous and Proximity Operations (RPO), which utilizes technologies that allow an ADR/OOS vehicle to locate, approach, engage, and/or capture the target object. Currently, the challenge is moving away from human-based servicing missions, such as the Hubble servicing missions, and moving towards more autonomous vehicles, where humans are not physically in space performing the servicing. As such, for the purpose of this paper OOS can be defined as any autonomous or semi-autonomous (human-in-the-loop or human-on-the-loop) system that engages with a spacecraft and provides refueling, repair, re-orbit, or upgrade services. ADR systems can be defined as any system that removes or neutralizes space debris. The number of active and non-active satellites, rocket bodies, remnants of collisions, and debris objects from new collisions is only expected to increase, so a variety of systems will eventually need to be deployed to mitigate and remove the debris threat. OOS may end up being less prevalent than ADR, but if a commercial servicing market emerges, or if servicing technology becomes reliable and significantly cheaper than new satellite systems, there may be a drastic increase in operational OOS systems.

The intimate and intrusive nature of ADR/OOS/RPO systems has given rise to concerns that the technology could be misused for nefarious purposes. For the purposes of this paper, misuse is defined as the full or partial deliberate destruction or disablement of a satellite system and/or satellite capability, *carried out under the guise of normal operations*. Misuse *could be conducted intentionally* by the ADR/OOS system through deliberate design, *or unintentionally*, through external influence like sabotage or cyberattack. Additionally, this definition *assumes no use of traditional weapons or ordnance* and refers strictly to misuse of the servicing spacecraft and its operations. While there is certainly the potential for these systems to be armed in a manner that includes conventional weapons, those concerns lie outside the scope of this paper, which assumes a standard OOS/ADR system. Such misuse could be initiated intentionally by a covert provider, or unintentionally by an outside influence like sabotage or cyberattack. In either of these cases, the benign ADR/OOS system would then become a space-based anti-satellite (ASAT) system, defined as systems that are utilized as a weapon to destroy, damage, or disable operational satellites. There are existing and proposed policies that have some influence on ADR/OOS operations, but they are currently either not clearly defined or not robust enough to have enough direct impact to assuage misuse concerns. Some policies, such as the proposed Prevention of an Arms Race in Outer Space (PAROS) treaty and the International Code of Conduct for Outer Space Activities, are stalled in the negotiation phase, with significant progress unlikely because of geopolitical tensions. Some actors, such as the United States, have internally begun developing related policy and definitions of norms. Such action is promising, but more is required to begin building an agreeable international framework for ADR/OOS/RPO. This paper captures the research effort to understand the current state of misuse concerns among a variety of subject matter experts and, combined with a policy and literature analysis, provides recommendations for SWF actions and positions.

Key Findings

- While ADR/OOS/RPO technologies could technically be used for nefarious purposes, it is unlikely that hostilities would be carried out under the guise of normal benign servicing operations.
- The concept is unrealistic because behavioral norms, standardized processes, and a robust SSA framework would immediately identify any deviation from such. These mitigating factors are expected to evolve in parallel with any servicing market.
- Because of the high likelihood of attribution and difficulty of deniability, misuse of benign servicing systems presents a high geopolitical risk to state actors.
- The experts that were interviewed for this analysis found the attribution factor so significant that they did not provide any probability of misuse estimates, mainly because of the drastic shift required in geopolitical climate before any valuable probability metric could be established.
- The areas of real concern were not related to any direct ASAT attack, but the covert use of private servicing missions for non-servicing national security purposes, or the suspicion of less-advanced space faring states leading to misinterpretation or conflict.

Recommendations

Based on this analysis and the key findings, this report presents recommendations for further actions. The Secure World Foundation should:

- Continue to help build norms at both the domestic and international level, providing all space actors the ability to discern intent of a servicing mission well in advance. This can be achieved through continued CONFERS support and coordination with all stakeholders.
- As the satellite servicing market and RPO evolves, support the incorporation of established norms into more legally-binding and/or regulatory systems.
- Even though efforts for a universal agreement have been difficult in the past, facilitate multi-lateral adoption of these norms.
- Encourage transparency from ADR/OOS/RPO operators, which would facilitate validation of behavior norm compliance and establish framework integrity.
- Most importantly, encourage and advocate for the development and improvement of space situational awareness (SSA) capabilities, which will provide a publicly available and multilateral avenue for the enforcement and verification of adherence to standards and norms.

Introduction to Problem

Technical Overview

In order to understand the concern that arises from ADR and OOS technologies some basic understanding of the technologies themselves must first be understood. As such, it is a worthwhile endeavor to introduce a number of technologies under development or in conceptual consideration. Additionally, beyond the technologies themselves, defining the general requirements for operations of ADR and OOS systems will help set the foundation for policies that could begin to address concerns related to RPO technologies. The following discussion is not intended to be an exhaustive list of technologies and their operational implementations, but will set the stage for the major concerns associated with these technologies.

All OOS or ADR systems will require RPO technologies in order to operate. RPO capabilities require a group of camera and/or radar technologies (e.g. visible cameras, infrared cameras, LIDAR, radar imaging, radar), the ability to process the data from these technologies in near real-time, as well as propulsive capabilities to maneuver along very defined, near-target trajectories. Resulting from the use of imaging technologies in close proximity, systems with RPO payloads can “see” the objects they are maneuvering around. This alone raises a concern amongst some stakeholders that these systems may “see” something they should not, providing the potential to use these satellites for government- or commercially-based espionage, providing adversaries with the ability to reverse-engineer satellite technologies. While this is a concern in itself, the primary concerns for RPO-enabled systems arise from other activities that may be performed while in close proximity to other systems.

The additional types of activities that could be performed while in proximity to other systems in space are numerous, and are based on the other types of technologies (OOS and ADR mission-specific technologies) attached to those systems. To provide a few examples:

- Communication payloads could be repurposed as a means of jamming a satellite up close

- Harpoons could be shot towards other systems to disable certain subsystems or the entire satellite
- Grappling technologies could be used in tandem with on-board toolsets to disable a satellite
- Grappling technologies could also be used in concert with propulsive technologies to move the system into a different orbit or to de-orbit it, making the system unusable or lost

Each of these concepts could be implemented in a number of ways depending on the technologies on-board the ADR or OOS systems. While none of these concepts are truly new or revolutionary for space-based systems, the increased levels of development, automation, and proliferation of these technologies has instilled additional levels of fears in current space actors.

On the operational side of OOS or ADR systems, mission operations include at least the segments of launch, several different orbital maneuvers, proximity operations, rendezvous, and docking (including capture or attachment). For ADR systems this may also include deorbit or graveyard maneuvers. Of these operational segments, the most potentially concerning are the proximity operations, rendezvous, docking, and de-orbit segments, wherein many of the aforementioned nefarious activities could occur. A single OOS or ADR operation of the servicing system, from orbit maneuver initiation until mission completion, is likely to take anywhere between 4 and 14 hours, with an approximate average time of 7 hours.[1] As defined, this timeframe actually doesn't include launch, because when these systems become more common it is likely that they will be injected in holding orbits until an OOS or ADR operation is required. Understanding the time boundaries of such activities is an important aspect of these technologies that should not be overlooked.

Since a single operation can take anywhere between 4 and 14 hours, it is fairly obvious that these operations are not rapid events. Completion of orbital maneuvers, identification, and pursuit of a target system requires constant maintenance, whether autonomously or by humans-on-the-loop, in order to accomplish these missions. As such, these requirements necessitate longer timelines. This gives target system operators the time to understand that another system is potentially approaching them. On the flip

[1] Colmenarejo et al., "GNC Aspects for Active Debris Removal."

side, since this timeline doesn't include the launch phase, if longer times exist between launch and orbital maneuver initiation, especially if tracking for the system is non-continuous, attribution (i.e. identification of ownership) of the potentially hostile actor may be harder to accomplish. The importance of these points will become more apparent during the discussion of potential policy options for RPO-based systems.

Current Space Environment and RPO Efforts

Before detailing the concerns surrounding RPO-based technologies, it is valuable to examine the catalyst for the development of these systems. For the majority of the Space Age, the space domain has been dominated by two primary actors, the governments of the United States and Soviet Union. Since the fall of the Soviet Union, numerous other government and commercial actors have also become space actors. As a result, the space domain is currently characterized by the U.S. national security apparatus as congested, contested, and competitive.[2] In this new paradigm, the effects of man-made space debris have become an increasingly important issue, leading to increased advocacy for advances in OOS and ADR systems. The mitigation and removal of space debris is a central impetus behind the technologies' development. OOS systems provide the ability to extend the life of these systems, decreasing the amount of non-operational systems in space as well as the need to launch new systems, while ADR provides the ability to remove current and future pieces of debris, decreasing the risk space debris poses to operational spacecraft.

Space debris, and the understanding of the risk involved, first became a larger consideration in the space community following the release of a paper in 1978 by Donald J. Kessler and Burton G. Cour-Palais entitled "Collision Frequency of Artificial Satellites: The Creation of a Debris Belt." Their paper concluded that as humans continue to send up satellites, the probability of collisions between satellites and debris already in orbit will also increase. These collisions in turn will create more debris, increasing the probability of more collisions, and so on. This idea eventually became known as the Kessler Effect (or

[2] US Department of Defense, "National Security Space Strategy [Unclassified Summary]."

Kessler Syndrome), wherein operating in the space environment becomes costly because of cascading debris clouds, created by a chain reaction of collisions.[3] Some believe our space environment has already moved beyond the point of no return regarding the Kessler Effect.[4]

Whether this is true or not, the ideas presented in the Kessler paper have convinced many that space can no longer be considered infinite, as was previously believed. This primarily arises from the fact that space actors tend to limit themselves to those orbits that are most beneficial to the intended mission. This effectively makes space, specifically near-Earth space, a limited resource. This argument is especially true for the geosynchronous equatorial orbit (GEO). A geosynchronous equatorial orbit is a specific orbit that is a circular geosynchronous orbit, which is located 35,786 km (22,236 mi) above Earth's equator. These orbits also follow the direction of Earth's rotation, thus a satellite in GEO appears fixed in the sky above to ground observers. Many space actors utilize this unique property of GEO, making the GEO belt a highly concentrated area of space, and thus it is considered by a scarce resource.[5]

Since the release of the Kessler-Cour-Palais paper, the largest additional investment and improvement in debris-related capabilities has come in the form of updated and expanded space situational awareness (SSA). Space situational awareness, as defined by the U.S. Joint Publication 3-14 Space Operations, is:

> "the requisite foundational, current, and predictive knowledge and characterization of space objects and the operational environment upon which space operations depend – including physical, virtual, information, and human dimensions – as well as all factors, activities, and events of all entities conducting, or preparing to conduct, space operations."[6]

This capability is then further divided into the four sub-capabilities of Detect/Track/Identify, Threat Warning and Assessment, Characterization, and Data Integration and Exploitation. Based on this definition, for any legitimate space debris policy and/or operation, SSA is always a necessity, a backbone

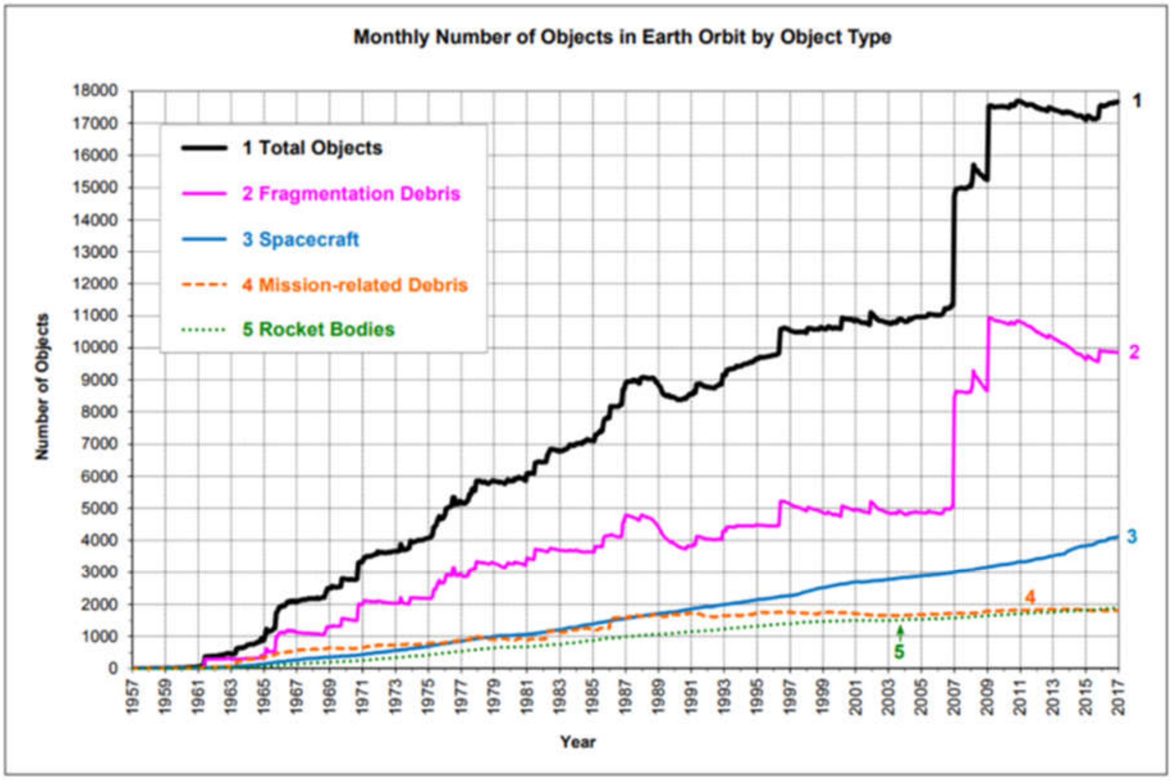
---

[3] Kessler, Donald J., and Cour-Palais, "Collision Frequency of Artificial Satellites: The Creation of a Debris Belt."
[4] Broad, "Orbiting Junk, Once a Nuisance, Is Now a Threat."
[5] Finch, "Limited Space: Allocating the Geostationary Orbit."
[6] US Air Force, Annex 3-14 Counterspace Operations, Space Situational Awareness.

that enables use of these technologies by identifying space objects and their ownership, which could then be utilized to define potential targets.[7]

In more recent events, in January 2007, the Chinese government conducted an ASAT test, specifically a ground-launched ASAT, destroying one of its own weather satellites in Low Earth Orbit (LEO), approximately 860 km above the Earth. Additionally, nearly two years later, another large space debris generation event occurred in February 2009, when the Russian Cosmos 2251 satellite and the commercial (US-based) Iridium 33 satellite collided. At the time, the Russian satellite was no longer operational, but the Iridium satellite was. This collision occurred at approximately 800 km above Earth in LEO, relatively close in altitude to where the Chinese ASAT test occurred two year later. Figure 1~~Figure 1~~ below shows the effect of the 2007 and 2009 debris generation events, an increase in trackable debris pieces of almost 80%. These two occurrences, close to one another in both time and orbit, effectively neutralized any positive effects that the previous adherence to debris mitigation standards may have had (this refers to Orbital Debris Mitigation Standard Practices, to be defined later).

[7] Ibid



Monthly Number of Cataloged Objects in Earth Orbit by Object Type: This chart displays a summary of all objects in Earth orbit officially cataloged by the U.S. Space Surveillance Network. "Fragmentation debris" includes satellite breakup debris and anomalous event debris, while "mission-related debris" includes all objects dispensed, separated, or released as part of the planned mission.

Figure 1. Monthly Number of Objects in Earth Orbit by Object Type[8]

Since these two events, advocacy for debris remediation techniques began to take shape. Many of the studies conducted since then have concluded that the path to remediation begins with the de-orbit of medium-to-large orbital debris pieces. As such, soon after the Chinese and Russian events, the U.S. Defense Advanced Research Projects Agency (DARPA) became interested in rendezvous and proximity operations (RPO) technologies. In 2009, DARPA began a study into ADR technology called "Catcher's Mitt" and participated with NASA in an international ADR workshop. The results of these projects recommended the continuation of ADR development.[9] While these projects were soon ended, DARPA began and continues to run the Consortium for Execution of Rendezvous and Servicing Operations (CONFERS) and its

[8] Liou, "Active Debris Removal and the Challenges for Environment Remediation."
[9] Defense Advanced Research Projects Agency, "Catcher's Mitt Final Report."

Robotic Servicing of Geosynchronous Satellite (RSGS) program, both of which are heavily grounded in partnership with aerospace industry.[10]

On the civil space of the U.S. government, NASA is currently developing Restore-L. This OOS project demonstrates the ability to rendezvous and service a non-cooperative satellite in LEO, specifically a refueling mission of Landsat-7.[11] Additionally, several other entities are performing research and development (R&D) on ADR technologies, including universities and commercial companies. In this group are developers such as RemoveDEBRIS, Astroscale, CleanSpace One, e.Deorbit, and The Aerospace Corp.[12]

RemoveDEBRIS, an initiative led by the University of Surrey alongside 10 international commercial partners, utilizes a net and a harpoon to catch debris and a solar sail to deorbit it. Astroscale's technology provides an end-of-life service wherein operators can use all of their available propulsion for their intended mission as opposed to saving some for de-orbit purposes. They can then buy a de-orbit service from Astroscale which will launch a small "chaser" satellite that will secure itself to dead satellites via magnets and then propulsively de-orbit both itself and the dead satellite. CleanSpace One is a project run by the École Polytechnique Fédérale de Lausanne to demonstrate capture and de-orbit of a partner CubeSat. This group expects to work with industry to eventually market their technology at a low cost. The European Space Agency (ESA) also has their e.Deorbit project, originally intended to remove the Envisat satellite, one of the largest pieces of debris in space. However, the project didn't receive funding in 2018/2019 and instead those funds were redirected to develop more synergy between ADR and OOS technologies. Finally, the Branecraft project, developed by Siegfried Janson at The Aerospace Corp., is expected to test several new technologies in the near future and hopes to find continued sponsorship after their testing is complete.[13]

---

[10] Recently the primary contractor for RSGS (Maxar) has had internal funding issues and pulled out of RSGS, DARPA has since decided to continue with the mission, but is looking for a new commercial partner
[11] Alessandro, "NASA's Restore-L Mission to Refuel Landsat 7, Demonstrate Crosscutting Technologies."
[12] Werner, "Rise of the Megaconstellations Breathes Life into Active Debris Removal Schemes."
[13] Werner.

While some of the entities performing ADR and OOS research are working on cooperative customers as a primary base, there are several instances of developing technologies for non-cooperative use, including the three projects run by government agencies (RSGS, Restore-L, and e.Deorbit). The logic for development of non-cooperative operations is simple: if a non-cooperative satellite can be serviced or de-orbited, then it would be much easier to perform the same operations with a cooperative satellite. These development efforts demonstrate an important concern many have regarding these technologies: their ability for dual-use purposes. The dual-use nature of these technologies adds to the concern over space-based ASATs, primarily stemming from direct military use or indirect misuse of these technologies. These space-based ASATs could potentially create a revolution in space affairs, moving the state of the space domain to an even more contested, and potentially an actively hostile, state.

Based on the current space environment and the manner in which RPO technologies achieve their mission, there is a notable level of political contention regarding these technologies. While many, if not all, space systems could be described as dual-use (i.e. used for either civilian or military purposes) these technologies seem to be more internationally politically contentious. The RPO technologies enabling the operational stages of proximity operations, rendezvous, contact/capture, and de-orbit are the primary targets of this contention. The capability to perform these operations make RPO systems some of the most advanced technologies in the space domain, ones that could be utilized as space-based anti-satellite (ASAT) systems.

To summarize the current RPO environment, the 2007 and 2009 debris generation events thoroughly magnified the threat posed by space debris. The number of current and near-future space actors has also jumped dramatically, leading to renewed interest in developing and deploying RPO, OOS, and ADR technologies by multiple governments and companies. To summarize the concerns that arise from these new developments, these technologies are inherently dual-use in nature. This has led to some viewing their use (or misuse) as a potential threat within the space domain.

Introduction to Current Policy Environment

The basic principles for international law in outer space were established by the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, more commonly known as the Outer Space Treaty. This document entered into effect in 1967 and establishes, among other provisions that countries may not place weapons of mass destruction in orbit or make claims of sovereignty over extraterrestrial bodies.

A number of specific provisions of the Outer Space Treaty are particularly relevant to RPO questions. First, parties to the treaty "bear international responsibility" for national actions in outer space, including activities conducted by non-government entities, and are obliged to authorize and continually supervise those actions to ensure they conform with international law. Second, parties to the treaty indefinitely retain jurisdiction over objects and their component parts launched into or built in space and registered by that country. Third, parties to the treaty are liable for damages caused by space objects under their jurisdiction, or launched in their territory, to other state parties and their natural and juridical persons. While the Outer Space Treaty prohibits the placement of weapons of mass destruction in orbit, no mention is made of conventional weapons systems.[14] The 1972 Liability Convention specified that states are absolutely liable for any damage caused within the atmosphere by space objects, but liable for damage in space only if they or entities under their jurisdiction are responsible.[15] A handful of other subsequent agreements modified or superseded elements of the original Outer Space Treaty for those countries that adopted them, but the above framework related to RPO remains fundamentally in place.

On multiple occasions since the passage of the Outer Space Treaty, states and activist groups have attempted to implement a ban on conventional weapons in space in addition to the Outer Space Treaty's ban on weapons of mass destruction. To this end, the International Conference on Disarmament has

---

[14] United Nations General Assembly, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies.
[15] United Nations General Assembly, "Convention on International Liability for Damage Caused by Space Objects."

periodically discussed a treaty for the Prevention of an Arms Race in Outer Space (PAROS) which would place limits on conventional weapons in space. To date these negotiations have proven ineffective, as the United States has expressed objections to treaty language put forward by Russia and China.[16] In particular, the United States has noted that negotiators have failed to produce an acceptable and unambiguous definition of a "weapon in outer space" that can be effectively verified without infringing on the ability to deploy inherently dual-use systems like ADR and OOS for peaceful purposes.[17] Critics have also noted that PAROS language prohibits weapons in space, but not ground-launched anti-satellite missiles, which along with the previously stated omissions make the treaty a "hollow exercise in public diplomacy."[18]

U.S. responses to proposed PAROS treaties have suggested that the task of creating meaningful definitions and effective verification regimes to limit conventional weapons in space is fundamentally impossible. Arguing against the need for a PAROS treaty in the first place, the United States has suggested that existing international law is sufficient to prevent the use of force against space objects. Instead of a comprehensive treaty banning conventional weapons, the U.S. has proposed bilateral and multilateral adoption of guidelines, norms of behavior, and the implementation of transparency and confidence-building maneuvers for space activities as sufficient steps to reassure states that other states are meeting their international obligations to avoid conflict in space.[19]

The International Code of Conduct for Outer Space Activities is one of the major active international effort to define norms and guidelines that would govern space activities in the absence of some other form of agreement. The International Code of Conduct is based on a European Union Code of Conduct agreed to by EU member states in 2008, which the EU subsequently submitted as a framework

[16] Nuclear Threat Intiative, "Proposed Prevention of an Arms Race in Space (PAROS) Treaty."
[17] Delegation of the United States of America, "Conference on Disarmament CD/2129."
[18] Krepon, "Space Code of Conduct Mugged in New York."
[19] Delegation of the United States of America, "Conference on Disarmament CD/2129."

for discussions with the international community. The EU's draft text has been the subject of a number of international meetings, and the text has been updated a number of times to reflect those discussions.[20]

The proposed International Code of Conduct seeks to improve the "safety, security, and sustainability" of activities in space and establish what are commonly called Transparency and Confidence Building Measures (TCBMs). TCBMS are a more recent method utilized in the international arena that enhance "mutual understanding and trust" and reinforce helpful norms in space. The code includes provisions that call for states to inform other parties about launches, maneuvers, malfunctions, and debris-creating events. The code also calls for participants to cooperate to avoid harmful interference between space objects, and to avoid actions that would cause damage to space objects or create space debris.[21] The text of the code provides minimal detail about the specific norms that would be established, but it suggests that the intent is for norms to would develop collaboratively from practical experience after nations have made a commitment to transparency and cooperation. In theory, a principle of transparency and a code of norms would allow states to distinguish between benign and malign actors in space. Instead of viewing every use of a dual-use technology like RPO and ADR as a threat, entities could focus their concern on space actors that are not in keeping with established norms or forthcoming about their actions.

Unfortunately for its advocates, the International Code of Conduct has also hit roadblocks for global implementation. At the end of a 2015 meeting, consideration of the Code was passed to the multilateral independent but UN-affiliated Conference on Disarmament, where PAROS treaties and other arms control agreements have languished for decades. The move was spearheaded by the Russian and Chinese delegations, with assistance from their allies in BRICS[22] and the remnants of the Cold War Non-Aligned Movement. The Russians and Chinese expressed concern that the Code preserved the UN

[20] Secure World Foundation, "Draft International Code of Conduct for Outer Space Activities Fact Sheet."
[21] European Union, "International Code of Conduct for Outer Space Activities and Space Debris Mitigation."
[22] Brazil, Russia, India, China, and South Africa (BRICS)

Charter's language about a state's right to self-defense rather than prohibiting military action in space entirely. Opponents of the Code also opined that the EU had unilaterally introduced its framework for the Code rather than eliciting the participation of developing countries and building broader consensus before formal negotiations began.[23] Though negotiations are still technically ongoing, the relegation of these discussions to the Conference on Disarmament has led some to conclude that multi-lateral approaches to these topics are non-viable for now.[24]

With little movement in the international arena, some countries, like the United States, have begun efforts to build operational norms internally. The Defense Advanced Research Projects Agency (DARPA) established the Consortium for Execution of Rendezvous and Servicing Operations (CONFERS) in August 2016. This group includes government agencies, space companies, and insurance firms and is intended to develop optional standards and best practices for responsible behavior for RPO and OOS activities.[25]

CONFERS began operations in August 2018, and released its first major document, outlining "guiding principles for commercial rendezvous and proximity operations and on-orbit servicing", in November 2018. The four principles outlined in the document CONFERS members agreed to begin with consent between owners of space assets prior to rendezvous. Second, members committed to complying with international law and the national laws relevant to both parties in the servicing activity. Third, members agreed to conduct responsible operations, including following generally accepted engineering practices, "reasonable provisions" for collision and debris creation mitigation, maintaining communication between servicer and client, insuring against risk to third parties, and waiting to establish standards and best practices until operational experience has built up. Finally, the parties also committed

---

[23] Krepon, "Space Code of Conduct Mugged in New York."
[24] Foust, "Trump Administration Continues Support of Outer Space Norms of Behavior."
[25] Defense Advanced Research Projects Agency, "Consortium for Execution of Rendezvous and Servicing Operations (CONFERS)."

to transparency with the governments with jurisdiction over servicers and clients as well as entities that could potentially experience harmful interference as a result of servicing activities, informing the public about anomalies and mishaps, and sharing lessons learned with other operators while respecting intellectual property, export controls, and trade secrets.[26]

In addition to producing policy documents, CONFERS also intends to act as an ongoing forum for discussing best practices and co-operating on RPO issues.[27] With further operational experience to validate best practices, CONFERS members will be able to craft more robust and specific technical and operational standards in a collaborative manner.

Methodology

The authors approached the problem with the hopes of gathering both qualitative and quantitative measures. The framework of the research effort was intended to solicit expert input regarding the potential scope of the problem, and there was an attempt to provide a preliminary quantified assessment of the risk and impact of misuse. Therefore, the research effort was centered around Subject Matter Expert (SME) interviews, as well as responses to a survey that presented both qualitative and quantitative inquiries regarding misuse of ADR/OOS/RPO technologies.

The survey was developed as both an interview guide and a fillable document that SMEs would return to the authors. After a brief introduction of the problem, the survey first asked for the respondent's initial thoughts on the validity of the problem. This was intended to capture a baseline qualitative reference before the in-depth exploration of possibilities began. The survey then presented a collection of scenarios of misuse, which intended to provide guiding examples of the situations that the research effort was attempting to explore. The scenarios helped frame the respondents' formulation approach to

[26] Consortium for Execution of Rendezvous and Servicing Operations, "Guiding Principles for Commercial Rendezvous and Proximity Operations (RPO) and On-Orbit Servicing (OOS)."
[27] Consortium for Execution of Rendezvous and Servicing Operations, "About."

the subsequent survey questions and provided a vision of far-future situations in which misuse could be probable, including some examples of misuse that may not have been initially apparent in a current-state context. The scenarios intended to prompt contemplation on the impacts of misuse, and what solutions could be put in place to mitigate it. Within the survey the respondents were reminded that the scenarios were just select examples, and they were encouraged to consider and imagine other misuse situations.

A definition for misuse, which is the full or partial deliberate destruction or disablement of a satellite system and/or satellite capability, carried out under the guise of normal operations was then provided to the respondents. This definition included the point that misuse could be conducted intentionally by the ADR/OOS system through deliberate design, or unintentionally through external influence like sabotage or cyberattack, and that the definition assumed no use of traditional weapons or ordnance and referred strictly to misuse of the servicing spacecraft and its operations. The survey also provided a definition for 'target object', which was defined as the spacecraft or object that is the intended recipient of ADR/OOS activities. However, the point was made that misuse could alternately target a different object for damage.

The survey then transitioned to a quantitative attempt to develop misuse metrics. The respondents were presented with a series of operational stages, most of them common to all ADR/OOS/RPO systems and asked to rank the realistic probability of misuse during each stage. The survey used a single digit estimate ranking between 1-5, with 1 meaning misuse was extremely unrealistic during that stage, and 5 meaning misuse was extremely realistic during that stage. Respondents were asked not to limit their considerations to traditional hostile actors like adversarial governments or militaries, but to consider all possible actors and scenarios that they deemed feasible at the future time that these systems would be operational. The survey then assessed critical impact of misuse with a similar ranking system. For this estimate, it was assumed that misuse of some type has occurred during the given operational stage, causing some level of damage or disablement to the target object. The respondents were asked to rank their estimate of operational impact from misuse during each stage, again using a single digit estimate, with 1 meaning that misuse would have no impact on a satellite's operations or capabilities, and 5 meaning that misuse would certainly cause complete destruction or irreversible disablement of the satellite and/or its capabilities.

The survey then returned to a qualitative discussion on specific technologies that may enable the potential misuse and how, particularly for any estimate that was rated at 3 or higher. The respondents were asked to discuss any mitigation solutions, including policies, pre-launch processes, and/or operational procedures, that could deter or prevent misuse and/or reduce impact. The survey ended with an opportunity for the respondent to provide closing thoughts or additional insight, reflecting on their initial thoughts provided at the beginning of the survey.

The responses to the quantitative portions of the survey were initially intended to be aggregated into a simple matrix, showing the average response for each operational stage's realistic probability of misuse vs the stage's potential operational impact if misused occurred. The matrix was intended to provide an easily digestible representation of the problem, and where mitigations efforts should be focused, as operations that are both highly susceptible to misuse and of high impact criticality would be visually evident. Because of the lack of response to the quantitative portions, for reasons to be discussed in the next section, the matrix was ultimately not created for this report.

Argument Assessment

The basis of any misuse concern lies in the inherent intimacy of ADR/OOS/RPO technologies. Currently, the only instance of close proximity operations occurs when crew or cargo capsules dock with the ISS. The process is comfortably familiar, as modern docking operations have existed in some form since the 1960s. The launches and missions that eventually rendezvous with the ISS are planned for months or years in advance, and are monitored from the moment of launch vehicle ignition through the opening of the docked capsule's hatch. While the process can be mostly autonomous, there is still real-time human control and observation. In short, there is no real scenario in the current space environment in which a fully autonomous system would approach the station or any other operational spacecraft without the entire world seeing it. Therefore, with ADR/OOS/RPO technologies soon to be operating on-orbit, finding, tracking, approaching, and touching orbiting spacecraft, there has been some stated concern that these systems could enable ASAT activities or lead to misperceptions and possible conflict. On the other hand, some feel that satellite systems and operational behaviors designed for benign RPO activities are not particularly well-suited to weaponization. On the surface, the core RPO technologies that ADR/OOS require for operations are inherently dual-use. The propulsion systems, navigation and guidance, and sensing technologies would be fundamentally identical for both benign and militarized implementations of satellite technologies. Technologically, there is no dispute that these systems could be repurposed for intentional harmful use, however that is not relevant to the analysis in this paper, because the concern of misuse is exclusive to benign servicing systems (intentional weaponization of these technologies is not misuse, as hostile acts *are* the intended use).

The counterargument to misuse concerns, and the unanimous position of the experts interviewed, is that when these systems go operational, there will be enough mitigating factors in place to make the misuse of ADR/OOS/RPO technology a terminally unattractive option for ASAT attacks. Firstly, any hostile actor that aims to misuse these services will find it nearly impossible to avoid attribution. Satellite systems, especially the non-stealth systems that ADR/OOS/RPO would be, are observable and trackable from launch. If a spacecraft attempts to deviate from its original target, it would be immediately clear to the new target's operator where the servicer came from, when it will intercept, and more critically, who owns it. Additionally, the attribution mitigation factor would likely be stronger in a future when these RPO systems are commonplace, as SSA data will then be more refined, more accurate, and more widely used, being built into the monitoring and verification processes of behavioral norm enforcement.

Another factor is the availability of alternatives. ASAT systems, both ground-based and co-orbital, already exist. These systems are designed for stealth and rapid deployment, or direct and open engagement, and in virtually all cases would be more lethally effective than a repurposed servicing spacecraft. Again, this factor is only strengthened in later decades as ASAT technology would likely be a more common tool for military deterrence. ASAT alternatives also have attribution impacts, as there is likely a better chance of avoiding detection employing a stealth weapon system instead of an SSA-observable servicing spacecraft. Lastly, the servicing technology and environment will evolve in parallel with the development of sufficient behavioral rules and processes. These norms would mostly eliminate the concern of misperception, in which space actors wrongly identify benign RPO activities as threats, by offering inclusion in a shared SSA framework with independent and multi-party verification.

A notable key finding from the survey-driven research effort was the similar response to the quantitative estimation questions. Every expert that was interviewed expressed concerns of the value of trying to capture probability metrics for such unlikely events, with some experts poignantly stating that the international stage would have to shift drastically before it was even worth discussing probability. This is a relevant outlook for the counterargument. The certainty of detection and attribution would make RPO misuse a high-risk venture for any spacefaring nation, and the geopolitical climate is simply not conducive to taking such a risk, nor will it likely be anytime soon. Contemporarily speaking, it would be the equivalent of a country sending a uniformed military officer on a diplomatic mission to another country just to attempt a public assassination. Again, in the face of definitive attribution, an intentional stealth ASAT system is more effective choice.

There was one concern that most of the experts conceded as a possibility: hostile nation-states, especially those in which private industry and government overlap, could covertly use private servicing missions for non-servicing purposes. This doesn’t necessarily suggest misuse for ASAT purposes, but more likely for surveillance, targeting, or other national security operations. Concurrently, states that do not have a robust domestic private space sector may assume that private servicing entities from more hegemonic states are acting under government authority, creating the potential of tension and/or conflict. While norms can ameliorate some these concerns, there is more to be done in the realm of international agreements and more inclusive SSA frameworks.

Approach to Policy Solutions

Concerns over the misuse and potential weaponization of RPO, ADR, and OOS technologies center around the inherently dual-use nature of space systems and the difficulty of definitively ascertaining intent at a distance. If technologies cannot be effectively placed into “benign” and “harmful” categories, efforts to mitigate concerns over the misuse of RPO systems must center around demystifying intent.

Space actors need a way of discerning intent in advance, which can only be accomplished by monitoring behavior. A system of behavioral norms for RPO operations would give benign users a way to distinguish themselves from malicious users, making the task of discernment easier for entities making use of the space environment. In its role as a facilitator for the development of solutions to ensure space sustainability, the SWF would be well-advised to continue its work to help build these norms.

There are a number of different avenues through which norms can be built. Many of the more productive venues to pursue in the short term are unilateral mechanisms, developed within a single country or implemented within the RPO industry. Domestic norms can begin within the industry, with groups like CONFERS leading the charge. Working with RPO operators, satellite customers, insurers, and government stakeholders, the SWF can work to grow the CONFERS partnership to ensure buy-in, and use its role within the organization to help develop mutually agreeable, verifiable standards of behavior for these activities. Initially, as standards mature, it may be possible for them to be policed internally. Insurance policies could require adherence to norms, and satellite operators would likely select insured providers in order to protect their assets. Self-policing is not always ideal, but when industry knowledge in an emerging field evolves faster than the typically glacial pace of the regulatory process it may be necessary.

As the RPO industry matures, norm-building may move to more legally-binding systems. Government regulatory agencies could adopt established standards and industry best practices into the regulatory code, creating a more thorough enforcement environment than might exist in a self-policed setting. It is important, however, that regulators take care to follow standards set by the industry or work closely with stakeholders when designing binding requirements. Well-designed regulations can enhance the safety and security of the space environment, while poorly-designed ones have the potential to stifle the industry and inhibit innovation that might improve safety and security in the future.

Behavioral norms for RPO activities established within the United States could inspire governments or industry groups within other countries to adopt similar norms. Multinational insurers may require or strongly incentivize adherence to norms, or foreign companies might adopt them voluntarily in order to appear more trustworthy or responsible to potential clients. Conversely, there is a danger that overly restrictive binding regulations could encourage RPO operators to place themselves under the jurisdiction of countries with more relaxed standards. This phenomenon is comparable to "flags of convenience" on terrestrial seas, where ship owners will register their vessels with countries that have lower fees or weaker labor and environmental requirements in order to save costs. This phenomenon means that, perversely, attempts by countries to enforce stronger standards at sea often lead to lower overall adherence to those standards in the world market.[28] A similar dynamic in space would be extremely detrimental to security and sustainability, and it must be prevented by maintaining buy-in from RPO operators when developing any binding regulations. Achieving universal acceptance of behavioral

[28] Gregory, "Flags of Convenience: The Development of Opent Registries in the Global Maritime Business and Implications for Modern Seafarers."

requirements would also avoid the danger of flags of convenience, but truly global consensus appears illusive.

Supplemental to unilateral implementation of RPO behavioral norms, SWF should also work to facilitate multi-lateral adoption of these norms. Efforts to this end have already seen some level of success, such as the EU code of conduct negotiated between and approved by the countries of Europe.[29] Although most areas of the world lack international organizations as comprehensive as the European Union, there is value in pairs or groups of countries attempting to harmonize RPO norms between them. The United States and the European Union control approximately 93% of all satellite manufacturing revenues,[30] an indication of the clout that the two entities have within the space sector. Both being proactive about norm-building for RPO through CONFERS and the Code of Conduct has a huge impact on the industry as a whole, and an agreement between them could also be beneficial.

While negotiations between pairs or groups of countries to harmonize RPO behavioral norms would be valuable, a universal agreement seems unlikely. The International Code of Conduct, even with its loosely defined-norms, is seen as dead following its delegation to the moribund Conference on Disarmament.[31] This bodes poorly for future attempts at negotiating norms through international institutions like the UN, which will likely achieve the same fate unless a breakthrough can be made in Conference on Disarmament talks. Unilateral, bilateral, and multilateral agreements will all play some role in preserving the sustainability of the space environment, but unilateral and bilateral mechanisms are likely to be the most effective for implementing RPO norms in the near term.

Beyond the mechanisms used to develop norms, the norms themselves are vital to the success of any effort to alleviate concerns associated with the potential misuse of RPO technologies. The categories of norms identified by CONFERS' guiding principles is a solid framework for this discussion. Consent

---

[29] Secure World Foundation, "Draft International Code of Conduct for Outer Space Activities Fact Sheet."
[30] Bryce Space and Technology, "SIA Global Satellite Economy."
[31] Krepon, "Space Code of Conduct Mugged in New York."

between spacecraft owners, compliance with relevant law, “responsible behavior”, and transparency will all help to both make RPO safer and help concerned space actors distinguish operators who want to act responsibly from those that don’t.[32]

While compliance with the law is a straightforward norm, and norms of “responsible behavior” are expected to develop only after RPO operations can begin and best practices analyzed, there are a number of ideas that can be incorporated into the norms of transparency and consent now. For example, transparency can be enhanced by a commitment from RPO operators to notify the public of all of their maneuvers and intentions, which allows concerned observers to compare actual behavior with stated intentions and judge the operator’s sincerity. This can be further supported to a commitment to “anti-stealth,” avoiding technologies that would make a spacecraft harder to track and potentially incorporating technologies that actively broadcast a spacecraft’s motions. One possibility in this regard is a norm or requirement that satellites smaller than some tracking systems are capable of detecting carry a beacon or reflector system. As with the other norms discussed in this paper, it could be enforced by self-interested insurance companies, domestic regulatory agencies, or international organizations like the International Telecommunications Union which currently govern and coordinate some aspects of space operations.[33]

The norm of consent can also be enhanced in a number of ways. Agreement between RPO operators and clients, and with the relevant regulatory agencies, is vital to a sustainable RPO industry. Further development of this norm could involve gaining consent from third parties who could be immediately impacted by a particular operation. One mechanism for this would be the establishment of safety bubbles of varying radii, essentially areas of controlled approach, around spacecraft. RPO systems coming within a certain distance of third-party spacecraft could be expected or required to notify satellite operators about their presence and intentions. RPO spacecraft coming within a smaller bubble could be

---

[32] Consortium for Execution of Rendezvous and Servicing Operations, “Guiding Principles for Commercial Rendezvous and Proximity Operations (RPO) and On-Orbit Servicing (OOS).”
[33] International Telecommunications Union, “Space Services Department (SSD).”

expected or required to gain consent from third-party satellite operators, which might alleviate concerns that a benign RPO system poses a threat. Standards for these safety bubbles could be based on the sizes of the uncertainty ellipses for a spacecraft's location used in the calculations for issuing warnings about potential collisions between space objects.[34]

Successful implementation of any of these norms and their value as a tool to discriminate between benign and malicious actors depends heavily on the capacity for independent verification of the movement of objects in space. This means that space actors, both governments and private entities, will need to develop and improve SSA capabilities, and the SWF should encourage that development. Presently, the U.S. military's Combined Space Operations Center (CSpOC) collects data on spacecraft positions and maneuvers and uses them to provide collision and close approach warnings to satellite operators around the world.[35] Space actors concerned that a U.S. or allied RPO satellite poses a security threat are unlikely to trust a U.S. military assessment of the risks such a satellite poses, and would likely be placated somewhat by an independent source of information that validates CSpOC data. A proliferation of SSA capabilities would reduce security concerns by allowing more space actors to feel they can trust available data, and help ensure that attribution of a malicious action in space can always be achieved. This supports both the enforcement of norms and the deterrence environment that comes from the knowledge that no malicious actor can hide their activities and go unpunished. Existing SSA data is limited in its utility by uncertainties in the position and movement of space objects.[36] Additional and more precise sources of information, when shared, could also improve the accuracy of SSA data for all users, ensuring that space actors get the information they need to make decisions without being inundated by false

---

[34] Hejduk and Pachura, "Conjunction Assessment Screening Volume Sizing and Event Filtering in Light of Natural Conjunction Event Development Behaviors."
[35] US Strategic Command, "U.S. Strategic Command Fact Sheet Combined Space Operations Center / 614th Air Operations Center."
[36] Hejduk and Pachura, "Conjunction Assessment Screening Volume Sizing and Event Filtering in Light of Natural Conjunction Event Development Behaviors."

alarms and irrelevant data. SWF would be well-advised to use its role as a facilitator of discussions to bring stakeholders together to share SSA data for mutual benefit.

Conclusion

RPO technologies and their utilization provide examples of legitimate concern amongst space actors. The increased development of ADR and OOS systems in response to the more populous space environment, of debris and operational actors alike, have magnified those concerns as these types of operations become more autonomous in nature. It was the intent of this paper to alleviate those concerns amongst space actors, specifically regarding the misuse of these technologies.

Within the international arena, several instances of multi-lateral policy development have been roadblocked for a number of reasons, some political in nature, others based on legitimate policy implementation concerns. This has led the United States to begin to develop policies regarding RPO-based systems domestically as the commercial sector continues to grow. The DARPA forum CONFERS is a good starting point to build norms and standards across government and industry actors. The research performed for this paper has found that operational norms revolving around operational intent is the most effective manner to regulate RPO activities. Attempts to ban technologies related to normal ADR or OOS operations is an ineffective manner, based on the inherent dual-use of the technologies involved.

Thus, working alongside CONFERS, SWF should continue to build norms based on concepts such as operational "keep-out" zones that define procedures for maneuvering and approach of target service receivers. These procedures will help identify between benign and malicious actors. Additionally, support for advanced space situational awareness, from commercial and government actors, is another method of reducing the risks involved with misuse of RPO-based systems. Having the capability to effectively identify and characterize operations undergoing within the space environment will allow for greater transparency in the intent related to those actions.

After domestic efforts have been achieved, the U.S. can utilize a number of forums for developing bilateral and potentially multi-lateral agreements with other space actors. SWF should continue to facilitate avenues for achieving these agreements while helping to build the U.S.'s domestic approach. The development and agreement of operational norms will be a large and time-consuming undertaking, but that should not stifle SWF or any other supporting organizations. For space sustainability to become a reality, space actors must continue to develop appropriate norms or operation.

Bibliography

Alejandro Earl, B. 2013. “Space Debris Mitigation CONOPS Development.” *Dissertation, US Air Force Institute of Technology*. https://apps.dtic.mil/dtic/tr/fulltext/u2/a581062.pdf.

Alessandro, Adrienne. 2016. “NASA’s Restore-L Mission to Refuel Landsat 7, Demonstrate Crosscutting Technologies.” NASA SpaceTech. 2016. https://www.nasa.gov/feature/nasa-s-restore-l-mission-to-refuel-landsat-7-demonstrate-crosscutting-technologies.

Barbee, Brent W., J. Russell Carpenter, Scott Heatwole, F. Landis Markley, Michael Moreau, Bo J. Naasz, and John Van Eepoel. 2011. “A Guidance and Navigation Strategy for Rendezvous and Proximity Operations with a Noncooperative Spacecraft in Geosynchronous Orbit.” *The Journal of the Astronautical Sciences* 58 (3): 389–408. https://doi.org/10.1007/bf03321176.

Baudet, Lucille, and Ruffiot, Manon. 2016. “Active Debris Removal: From the Main Barriers to the Definition of a Business Model.” http://chaire-sirius.eu/wp-content/uploads/2016/10/Ruffiot-Baudet-2016-Active-debris-removal-From-the-main-barriers-to-the-definition-of-a-business-model-Unknown.pdf.

Broad, William J. 2007. “Orbiting Junk, Once a Nuisance, Is Now a Threat.” *New York Times*, 2007. https://www.nytimes.com/2007/02/06/science/space/06orbi.html.

Bryce Space and Technology. 2017. “SIA Global Satellite Economy.” https://www.sia.org/wp-content/uploads/2017/07/SIA-SSIR-2017.pdf.

Choi, Charles Q. 2016. “China Says Work Under Way to Mitigate Space Junk.” Space.Com. 2016. https://www.space.com/4301-china-work-mitigate-space-junk.html.

Chow, Brian G. 2018. “Space Arms Control: A Hybrid Approach.” *Strategic Studies Quarterly* 12 (2): 107–32. https://www.jstor.org/stable/26430818?seq=1#metadata_info_tab_contents.

Colmenarejo, P., G. Binet, L. Strippoli, T.V. Peters, and M. Graziano. 2012. “GNC Aspects for Active Debris Removal.” In *EuroGNC 2013, 2nd CEAS Specialist Conference on Guidance, Navigation & Control, Delft University of Technology*, 758–76. https://aerospace-europe.eu/media/books/delft-0084.pdf.

Committee on the Peaceful Use of Outer Space. 2012. “Active Debris Removal-An Essential Mechanism for Ensuring the Safety and Sustainability of Outer Space; A Report of the International Interdisciplinary Congress on Space Debris Remediation and On-Orbit Satellite Servicing.” In *Scientific and Technical Subcommittee Forty-Ninth Session*. http://www.unoosa.org/pdf/limited/c1/AC105_C1_2012_CRP16E.pdf.

Consortium for Execution of Rendezvous and Servicing Operations. 2018. “Guiding Principles for Commercial Rendezvous and Proximity Operations (RPO) and On-Orbit Servicing (OOS).” https://www.satelliteconfers.org/wp-content/uploads/2018/11/CONFERS-Guiding-Principles_7Nov18.pdf.

Consortium for Execution of Rendezvous and Servicing Operations. 2018. “About.” https://www.satelliteconfers.org/about-us/.

Defense Advanced Research Projects Agency. n.d. “Consortium for Execution of Rendezvous and Servicing Operations (CONFERS).” https://www.darpa.mil/program/consortium-for-execution-of-rendezvous-and-servicing-operations.

Defense Advanced Research Projects Agency. n.d. “Catcher’s Mitt Final Report.” https://apps.dtic.mil/dtic/tr/fulltext/u2/1016641.pdf.

Delegation of the United States of America. 2018. “Conference on Disarmament CD/2129.” *Conference on Disarmament* 2129 (August): 6. www.unog.ch/.

European Union. 2014. “International Code of Conduct for Outer Space Activities and Space Debris Mitigation.” https://eeas.europa.eu/sites/eeas/files/space_code_conduct_draft_vers_31-march-2014_en.pdf.

Finch, Michael J. 1986. “Limited Space: Allocating the Geostationary Orbit.” *Northwestern Journal of International Law & Business* 7 (4): 788–802. https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1216&context=njilb.

Force, Melissa Kemper. n.d. “Overview of Active Space Debris Removal Issues.” American Bar Asssociation. https://www.americanbar.org/content/dam/aba/images/air_space/course/16symposium/sp16-2-overview-active-space-debris-removal-issues.pdf.

Foust, Jeff. 2018. “UN Committee Approves Space Sustainability Guidelines.” Space News. 2018. https://spacenews.com/un-committee-approves-space-sustainability-guidelines/.

Foust, Jeff. 2018. “Trump Administration Continues Support of Outer Space Norms of Behavior.” 2018. https://spacenews.com/trump-administration-continues-support-of-outer-space-norms-of-behavior/.

Gopalaswamy, Bharath, and Gaurav Kampani. 2014. “India and Space Weaponization: Why Space Debris Trumps Kinetic Energy Antisatellite Weapons as the Principal Threat to Satellites.” *India Review* 13 (1): 40–57. https://doi.org/10.1080/14736489.2014.873678.

Grego, Laura. 2012. “A History of Anti-Satellite Programs.” *Union of Concerned Scientists*. https://www.ucsusa.org/sites/default/files/legacy/assets/documents/nwgs/a-history-of-ASAT-programs_lo-res.pdf.

Gregory, William R. 2012. “Flags of Convenience: The Development of Opent Registries in the Global Maritime Business and Implications for Modern Seafarers.” Georgetown University. https://repository.library.georgetown.edu/bitstream/handle/10822/557688/Gregory_georgetown_0076M_11950.pdf.

Hall, Loretta. 2014. "The History of Space Debris." In *Embry-Riddle Aeronautical University, Space Traffic Management Conference*, 1–10. https://commons.erau.edu/cgi/viewcontent.cgi?article=1000&context=stm.

Hejduk, M. D., and D. A. Pachura. 2018. "Conjunction Assessment Screening Volume Sizing and Event Filtering in Light of Natural Conjunction Event Development Behaviors." *Advances in the Astronautical Sciences* 162: 869–84. https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20170007928.pdf.

Hildreth, Steven, and Allison Arnold. 2014. "Threats to U.S. National Security Interests in Space: Orbital Debris Mitigation and Removal." *Congressional Research Service*. https://www.hsdl.org/?view&did=748309.

Imburgia, Joseph S. 2011. "Space Debris and Its Threat To National Security: A Proposal for a Binding International Agreement To Clean Up the Junk." *Vanderbilt Journal of Transnational Law* 44: 589. https://wp0.vanderbilt.edu/wp-content/uploads/sites/78/Imburgia-FINAL-CR-pdf.pdf.

Inter-Agency Space Debris Coordination Committee. 2007. "IADC Space Debris Mitigation Guidelines." 2007. https://www.iadc-online.org/Documents/IADC-2002-01, IADC Space Debris Guidelines, Revision 1.pdf.

International Telecommunications Union. 2019. "Space Services Department (SSD)." 2019. https://www.itu.int/en/ITU-R/space/Pages/default.aspx.

Jasani, Bhupendra. n.d. "Space Assets and Emerging Threats." http://www.unoosa.org/pdf/SLW2016/Panel2/1_Jasani_-_Space_assets_and_threats_06082016.pdf.

Kervendal, Erwan, Thomas Chabot, and Keyvan Kanani. 2013. "GNC Challenges and Navigation Solutions for Active Debris Removal Mission." In *EuroGNC 2013, 2nd CEAS Specialist Conference on Guidance, Navigation & Control, Delft University of Technology,* 761–79. https://doi.org/10.1007/978-3-642-38253-6_43.

Kessler, Donald J., and Cour-Palais, Burton G. 1978. "Collision Frequency of Artificial Satellites: The Creation of a Debris Belt." *Journal of Geophysical Research* 83 (A6): 2637. https://doi.org/10.1029/ja083ia06p02637.

Krepon, Michael. 2015. "Space Code of Conduct Mugged in New York." 2015. http://www.armscontrolwonk.com/archive/404712/space-code-of-conduct-mugged-in-new-york/.

Lal, Bhavya, Asha Balakrishnan, Becaja M Caldwell, Reina S Buenconsejo, and Sara A Carioscia. 2018. "Global Trends in Space Situational Awareness (SSA) and Space Traffic Management (STM)." *Institute for Defense Analysis*. https://www.ida.org/idamedia/Corporate/Files/Publications/STPIPubs/2018/D-9074.pdf.

Liemer, Ross, and Christopher F. Chyba. 2010. "A Verifiable Limited Test Ban for Anti-Satellite Weapons." *The Washington Quarterly* 33 (3): 149–63. https://doi.org/10.1080/0163660x.2010.492346.

Liou, J.C. 2013. “Active Debris Removal and the Challenges for Environment Remediation.” https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20120013266.pdf.

Liou, J.C. 2011. “Engineering and Technology Challenges for Active Debris Removal.” In *4TH EUROPEAN CONFERENCE FOR AEROSPACE SCIENCES (EUCASS)*, 735–48. https://doi.org/10.1051/eucass/201304735.

Liou, J.C. 2009. “(Preprint) AAS 11-254 ACTIVE DEBRIS REMOVAL – A GRAND ENGINEERING CHALLENGE FOR THE TWENTY-FIRST CENTURY.” https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20110011986.pdf.

Meek, Phillip A. 2011. “Strategic (Military) Implications of Active Debris Removal (ADR) and On-Orbit Satellite Servicing (OOS).” https://www.mcgill.ca/iasl/files/iasl/sdc2011_32_meek.pdf.

NASA Orbital Debris Program Office. n.d. “Briefing to the NASA Advisory Council.” https://www.nasa.gov/sites/default/files/files/OrbitalDebrisProgramOffice.pdf.

National Aeronautics and Space Administration. 2010. “On-Orbit Satellite Servicing Study.” *Project Report - Goddard Space Flight Center*. https://sspd.gsfc.nasa.gov/images/NASA_Satellite Servicing_Project_Report_0511.pdf.

National Aeronautics and Space Administration. 2008. “History of On-Orbit Satellite Fragmentations.” Orbital Debris Program Office. 2008. https://orbitaldebris.jsc.nasa.gov/library/satellitefraghistory/tm-2008-214779.pdf.

Nuclear Threat Intiative. 2017. “Proposed Prevention of an Arms Race in Space (PAROS) Treaty.” 2017. www.nti.org/learn/treaties-and-regimes/proposed-prevention-arms-race-space-paros-treaty/.

Nyampong, Yaw O.M. 2013. “Legal and Regulatory Challenges to Active Debris Removal and On-Orbit Satellite Servicing Activities.” In *SWF/SSTA Conference on On-Orbit Satellite Servicing and Active Debris Removal: Opportunities and Challenges for the Space Sector*. https://swfound.org/media/101969/yaw-legal_regulatory_challenges.pdf.

Office of the President of the United States. 2010. *National Space Policy of the United States of America*. https://obamawhitehouse.archives.gov/sites/default/files/national_space_policy_6-28-10.pdf.

Office of the President of the United States. 2018. “President Donald J. Trump Is Unveiling an America First National Space Strategy.” 2018. https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-unveiling-america-first-national-space-strategy/.

Office of the President of the United States. 2018. *Space Policy Directive-3, National Space Traffic Management Policy*. https://www.whitehouse.gov/presidential-actions/space-policy-directive-3-national-space-traffic-management-policy/.

Office of the Under Secretary of Defense for Policy. 2012. “Sustainability and the National Security Space Strategy: An Approach to the Contested Environment.” In *International Symposium on Sustainable Space Development and Utilization for Humankind*.

https://archive.defense.gov/home/features/2011/0111_nsss/docs/International Symposium on Sustainable Space Development and Utilization for Humankind.pdf.

Pekkanen, Saadia. 2018. “Why Space Debris Cleanup Might Be a National Security Threat.” Phys.Org. 2018. https://phys.org/news/2018-11-space-debris-cleanup-national-threat.html.

Popova, Rada, and Volker Schaus. 2018. “The Legal Framework for Space Debris Remediation as a Tool for Sustainability in Outer Space.” *Aerospace* 5 (2): 55. https://doi.org/10.3390/aerospace5020055.

R, Ghadawala, and Singh B. 2016. “Commercial Aspects of Active Debris Removal: Technical and Legal Challenges.” *Journal of Aeronautics & Aerospace Engineering* 05 (01): 1–4. https://doi.org/10.4172/2168-9792.1000159.

Richards, Matthew G., Philip N. Springmann, and Michelle E. McVey. 2005. “Assessing the Challenges to a Geosynchronous Space Tug System.” *Modeling, Simulation, and Verification of Space-Based Systems II* 5799: 135. https://doi.org/10.1117/12.603975.

Secure World Foundation. 2018. “UN COPUOS Working Group on Space Sustainability Concludes Its Work with Agreement on 21 Guidelines.” 2018. https://swfound.org/news/all-news/2018/08/un-copuos-working-group-on-space-sustainability-concludes-its-work-with-agreement-on-21-guidelines.

Secure World Foundation. 2014. “Draft International Code of Conduct for Outer Space Activities Fact Sheet.” https://swfound.org/media/166384/swf_draft_international_code_of_conduct_for_outer_space_activities_fact_sheet_february_2014.pdf.

Sorge, Marlon. 2017. “Commercial Space Activity and It Impact on U.S. Space Debris Regulatory Structure.” Center for Space Policy and Strategy, The Aerospace Corporation. 2017. www.aerospace.org/policyorpolicy@aero.org.

Taylor, Rob, and Brian Rishikof. 2010. “Tools and Techniques for a Systematic Approach to Safe Rendezvous and Proximity Operations.” In *Fourth IAASS Conference*.

The Aerospace Corporation. 2018. “Danger: Orbital Debris.” 2018. https://aerospace.org/story/danger-orbital-debris.

The Aerospace Corporation. 2018. “Space Debris and Space Traffic Management.” 2018. https://aerospace.org/story/space-debris-and-space-traffic-management.

The White House Office of Science and Technology Policy. 1995. “Interagency Report on Orbital Debris.” https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20000011871.pdf.

Union of Concerned Scientists. 2019. “UCS Satellite Database.” 2019. https://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database#.XAanpGhKjmE.

United Nations General Assembly. 1967. “Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space.” 1967. http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introrescueagreement.html.

United Nations General Assembly. 1971. “Convention on International Liability for Damage Caused by Space Objects.” 1971. http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introliability-convention.html.

United Nations General Assembly. 1974. “Convention on Registration of Objects Launched into Outer Space.” 1974. http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introregistration-convention.html.

United Nations General Assembly. 1967. *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies*.

United Nations Office For Outer Space Affairs. 2010. “Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space.” http://www.unoosa.org/res/oosadoc/data/documents/2010/stspace/stspace49_0_html/st_space_49E.pdf.

US Air Force. 2018. *Annex 3-14 Counterspace Operations, Space Situational Awareness*. https://www.doctrine.af.mil/Portals/61/documents/Annex_3-14/3-14-D04-SPACE-SSA.pdf.

US Department of Defense. 2011. “National Security Space Strategy [Unclassified Summary],” 14. http://archive.defense.gov/home/features/2011/0111_nsss/docs/NationalSecuritySpaceStrategyUnclassifiedSummary_Jan2011.pdf.

US General Accounting Office. 1990. “Space Debris a Potential Threat to Space Station and Shuttle.” https://www.gao.gov/assets/150/148911.pdf.

US Office of the Director of National Intelligence. 2018. “Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community.” https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1845-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community.

US Strategic Command. 2018. “U.S. Strategic Command Fact Sheet Combined Space Operations Center / 614th Air Operations Center.” 2018. https://www.stratcom.mil/Portals/8/Documents/CSpOC_Factsheet_2018.pdf.

Weeden, Brian C., Tiffany Chow, Agnieszka Lukaszczyk, and Victoria A. Samson. 2013. “International Perspectives on On-Orbit Satellite Servicing and Active Debris Removal and Recommendations for a Sustainable Path,” 1–14. http://swfound.org/media/119604/IAC-13-E3.4.7-Presentation.pdf.

Weedon, Brian. 2017. “US Space Policy, Organizational Incentives, and Orbital Debris Removal.” 2017. http://www.thespacereview.com/article/3361/1.

Weedon, Brian. 2018. "Trends in Commercial Space Situational Awareness." 2018. https://swfound.org/media/206218/weeden_commercial_ssa_jun2018.pdf.

Weedon, Brian. 2013. "The Non-Technical Challenges of Active Debris Removal." https://swfound.org/media/100609/bw_adr_iaf_copuosstsc_feb112012.pdf.

Werner, Debra. 2018. "Rise of the Megaconstellations Breathes Life into Active Debris Removal Schemes." Space News. 2018. https://spacenews.com/rise-of-the-megaconstellations-breathes-life-into-active-debris-removal-schemes/.

Appendix A – SME Survey and Interview Guide

1. Initial Thoughts

Active Debris Removal (ADR) and On-Orbit Servicing (OOS) systems will both use Rendezvous and Proximity Operations (RPO) technology to maneuver orbital space, track and approach objects in orbit, and/or manipulate those objects in some way. Outside of previous anti-satellite weapons tests, these systems will be the first in history to autonomously and intentionally operate in close, "hands-on" proximity to other spacecraft, and there are concerns that the technology could be misused for hostile objectives.

What are your initial thoughts about the validity of these concerns regarding the potential misuse of ADR/OOS/RPO systems? (Ignore the current technology readiness of these systems, and assume full operational capability at some point in the future)

2. Example Scenarios

The following scenarios are intended as guiding examples of the situations that this survey is attempting to explore, and your responses to the questions ahead should be formulated with similar scenarios in mind. The intent is to envision future/far-future situations in which misuse would be most probable, what forms that misuse could take, what impacts that misuse would have, and what solutions could be put in place to mitigate it. Again, these are just example scenarios; you are encouraged to consider and imagine other situations.

- An OOS mission, carried out by a benign DoD contractor, is tasked with refueling a national security communications satellite. China sanctions an independent cyberattack against the servicing vehicle, and during its close approach to the target commsat, the hackers upload an errant command that burns all thrusters at once, turning the servicing vehicle into an impactor. The commsat is severely damaged from the impact and much of its capability is interrupted.

- Russia secretly funds and controls a private Russian ADR company. The company is contracted to de-orbit a dead Russian satellite. Instead, the dead satellite is steered into a collision course with a US imaging satellite. Russia claims the incident is an accident, and blames the private company.

- The subsidiary of a private satellite communications company offers ADR services specifically for on-orbit collision response, using a fleet of autonomous net and tether spacecraft. After a large rocket body slams into a non-operational PNT satellite, the subsidiary is dispatched to launch the same day and begin ADR operations. One of the net vehicles veers away from the debris zone during maneuvers, and several hours later, clips an unrelated communications satellite with its open net. The commsat is able to maintain attitude, but its solar panels are damaged. The reduced power significantly affects its bandwidth capacity. The commsat is owned by a competitor of the subsidiary's parent company. The subsidiary claims the incident was not intentional.

3. Realistic Probability of Misuse

For each of the following operational stages, please provide an estimate for realistic probability of misuse.

Misuse is defined for this survey as the full or partial deliberate destruction or disablement of a satellite system and/or satellite capability, carried out under the guise of normal operations. Misuse could be conducted intentionally by the ADR/OOS system through deliberate design, or unintentionally, through external influence like sabotage or cyberattack. This definition assumes no use of traditional weapons or ordinance and refers strictly to misuse of the servicing spacecraft and its operations.

Target object is defined for this survey as the spacecraft or object that is the intended recipient of ADR/OOS activities, however please keep in mind that misuse could alternately target a different object for damage.

Please use a single digit between 1-5 to rank your estimate as follows:

Misuse is... 1 = extremely unrealistic during this stage.

2 = unrealistic during this stage.

3 = realistic during this stage.

4 = very realistic during this stage.

5 = a near certainty during this stage.

Please do not limit your considerations to traditional hostile actors like adversarial governments or militaries. Consider all possible actors and scenarios that you deem feasible at the future time that these systems would be operational.

Launch

Realistic Probability of Misuse Estimate:

Deployment (separation from launch vehicle)

Realistic Probability of Misuse Estimate:

Orbital Maneuvers

Realistic Probability of Misuse Estimate:

Telemetry tracking and acquisition of target object, including remote sensing of target object

Realistic Probability of Misuse Estimate:

Approach maneuvers to target object

Realistic Probability of Misuse Estimate:

Capture/tethering of target object

Realistic Probability of Misuse Estimate:

OOS Activities (refueling, component manipulation, piercing/intrusion upon the satellite body)

Realistic Probability of Misuse Estimate:

ADR Activities (de-orbiting, orbital changes)

Realistic Probability of Misuse Estimate:

4. Critical Impact

For the same operational stages, please provide an estimate for severity of impact in the event of misuse. For this estimate, assume that misuse of some type has occurred during the stage, causing some level of damage or disablement to the target object. The type of misuse and level of damage is intentionally vague and left to your own ideas of potential.

Please use a single digit between 1-5 to rank your estimate as follows:

Misuse during this stage...

1 = could have no impact on a satellite's operations or capabilities.

2 = could have minor impact on a satellite's operations or capabilities.

3 = could have moderate impact on a satellite's operations or capabilities.

4 = could have major impact on a satellite's operations or capabilities.

5 = could certainly cause complete destruction or irreversible disablement of the satellite and/or its capabilities.

Launch

Impact of Misuse Estimate:

Deployment (separation from launch vehicle)

Impact of Misuse Estimate:

Orbital Maneuvers

Impact of Misuse Estimate:

Telemetry tracking and acquisition of target object, including remote sensing of target object

Impact of Misuse Estimate:

Approach maneuvers to target object

Impact of Misuse Estimate:

Capture/tethering of target object

Impact of Misuse Estimate:

OOS Activities (refueling, component manipulation, piercing/intrusion upon the satellite body)

Impact of Misuse Estimate:

ADR Activities (de-orbiting, orbital changes)

Impact of Misuse Estimate:

5. For any of the above estimates that you rated at a 3 or higher, please discuss any specifics about how misuse could be achieved/implemented. Please discuss specific technologies that may enable the potential misuse, and how.

6. For any of the above estimates that you rated at a 3 or higher, please discuss any mitigation solutions, including policies, pre-launch processes, and/or operational procedures, that could deter or prevent misuse and/or reduce impact.

7. Closing Thoughts

Please take this optional opportunity to provide any additional thoughts or insight you may have.