Compact Solutions for Detecting Space and Ground Based Optical Threats to Satellites

Cameron Dickinson & Sebastian Slaman
MDA Space Robotics & Operations
Piotr Jasiobedzki, Dennis Gregoris & Denise King
MDA Space Robotics & Operations

1. OVERVIEW

In recent years, there have been a rise in the prevalence of Anti-satellite (ASAT) incidents. These events range from temporary disruptions via sensor dazzling, to destructive tests and demonstrations. The increased relevance of ASAT technologies is brought about by the growth of the space industry as a whole in combination with the development of ASAT related technologies. Satellite rendezvous and proximity operation technologies developed for satellite-to-satellite maintenance may readily be adapted for ASAT attacks. Similarly, LIDAR (Light Detection and Ranging) and laser scanning technologies are akin to various laser-based ASAT attacks such as dazzling and spoofing.

Various potential laser-based ASAT attacks can originate from adversarial ground stations or satellites, threatening satellites in any orbit. High-powered destructive laser attacks use IR lasers originating from ground stations, having effective ranges under 1000 km. Disruptive attacks such as dazzling, jamming, and spoofing can originate from a ground station or satellite, with effective ranges over 1000 km. The laser wavelength is dependent on the sensors of the target satellite it is trying to disrupt. Scanning and targeting based attacks such as LIDAR, laser rangefinders, or laser target designators tend to operate in the visible through to the near IR regimes and would have a limited range of a few hundred kilometres based on current technologies.

The rise in ASAT capabilities demands the development of protective measures for valuable satellite assets. The present work proposes a Detection Of Laser Operations in Space (DOLOS) system as a satellite protection technology. The system would be capable of monitoring lasers targeted at the satellite, determining the incoming wavelength, pulse pattern, direction of the laser threat source, and exact time of such event. By doing so, DOLOS would be able to detect and characterize incoming attacks as well as inform the satellite operator about them and enable attribution to specific sources in space or on the ground.

DOLOS is designed to operate using a collection of detectors covering multiple wavelength bands to sense incoming laser signals over a wide field of view. DOLOS will be able to identify the modulation and wavelength of an incoming signal. After this initial identification process, DOLOS will localize the signal source within the field of view, comparing all received signal measurements. Based on this data, the DOLOS search algorithm will be able to identify the source location. The incoming signal wavelength, modulation, intensity, exact time of the incident, and location data would then be forwarded to the satellite operator.

2. BACKGROUND

Satellites are vulnerable to a range of threats from adversaries that may deny or disrupt the operations of space assets or destroy them. Such threats may be posed by adversaries' satellites placed on similar orbits, increasing the likelihood of intercepting, jamming communications, or interfering with operations. Satellites have been destroyed from the ground using lasers or kinetic weapons, e.g., Indian anti-satellite weapon test in 2019, Chinese Anti-satellite (ASAT) test in 2007 or USA-193 in 2008. LEO through to GEO satellites are currently vulnerable to kinetic attacks. To detect and counteract such threats western democracies have initiated several programs: US Self Awareness/Space Situation Awareness (SASSA), US Bodyguard satellites protecting valuable assets, France – a new ASAT program including equipping satellites with Situational Awareness cameras and ability to dazzle threatening adversaries with lasers.

Laser Warning Systems (LWR) have been under development for many years for terrestrial defense applications [1] and have been deployed on military land vehicles and aircraft. They can detect incoming laser illumination at selected wavelengths at distances of up to several kms, can identify a sector where the source might be located but cannot identify the type of threat. The system under development at MDA uses similar principles of detecting monochromatic laser light and extends them into space domain. New features include determination of source characteristics, wavelength, irradiation and illumination directionality, thus providing satellite operators with the ability to locate and attribute the threat to a specific source. The system under development will operate at significantly longer rages that any terrestrial systems and in a hazardous space environment

The proposed solution, Detection Of Laser Operations in Space (DOLOS), will detect, characterize and localize threats posed to satellites by space and ground based lasers such as illuminators, designators, and rangefinders. This will provide intelligence to the satellite operators on potential adversary co-orbital and/or ground-based laser emitters. Such intelligence includes laser wavelength, pulse pattern, and intensity, as well as the exact time of the incident and directionality (location) of the threat emitter. This research has been funded through the Canadian Department of Defenses' IDEAS program.

There is a multitude of different ground- and spacebased laser ASAT threats from laser rangefinders to high-powered destructive lasers that threaten the functionality and wellbeing of a satellite [2]. Satellites are valuable assets that are highly vulnerable to such attacks. It is therefore vital to be able to detect and characterize such threats. To design a system that detect these threats, the general nature and characteristics of such threats need to be first understood.

The general types of laser-based attack vectors are sensing, jamming, spoofing, dazzling, blinding, and high-powered laser [2]. The laser ASAT weapon technologies would be based on current laser technologies used by the military. Table 1 presents a variety of different laser sources and their related military uses as examples of pre-existing technology associated with various potential ASAT attacks.

Table 1: Lasers Used in the Military and Their Purpose [3]

Laser Type	Wavelength	Purpose	Modulation	Power
Neodymium-doped Yttrium Aluminum Garnet (Nd:YAG)	0.532 µm / 1.06 µm	Atmospheric Communication	Q-switched / CW / Pulsed	0.5 - 1000 W
	1.06 µm	LRF/LTD	Pulsed	0.5 - 1000 W
	1.06 µm	LADAR	Q-switched / Pulsed	0.5 - 1000 W
	1.064 µm	Illuminator	Pulsed	up to 10's of Watts
	1.064 µm	Sensor	CW / Pulsed	up to 10's of Watts
Tunable laser Titanium Sapphire (Ti:S)	0.66 µm - 1.18 µm	Atmospheric Communication	CW	0.1 - few Watts
Gallium-Arsenide (GaAs)	0.85 µm	LADAR	CW / Pulsed	> 10 W
	0.83 µm	Illuminator	Pulsed	up to 10's of Watts
Raman-Shifted Nd:YAG	1.54 µm - 1.55 µm	LIDAR	Pulsed	> 10 W
Indium Gallium Arsenide (InGaAs)	1.55 µm	Illuminator	Pulsed	up to few Watts
Carbon dioxide (CO_2)	10.59 µm / 11.17 µm	Long-range LADAR	CW / Pulsed	4 kW to 5 kW peak
	9 µm - 12 µm	Weapon	CW / Pulsed	>100 kW

A high-powered laser strong enough to damage or destroy its target could be difficult to characterize prior to complete destruction – i.e., accurately detecting and localizing the incoming beam before the detection system is damaged.

However, a high-powered laser could require a secondary targeting and tracking system such as a laser target designator (LTD), laser rangefinder (LRF), or(LIDAR unit to keep the high-powered laser focused on the target satellite. Because of this, a laser detection system onboard the target satellite need not detect the high-powered laser itself directly and could just detect the targeting system used by the ASAT weapon.

3. CURRENT ASAT THREATS

Lasers for Sensing and Targeting

LTD, LIDARs, and LRF systems are similar in their functionality. In principle, they all work by directing laser light towards a target or object to locate it by measuring the reflected pulse signal. Contrary to dazzling, jamming, and spoofing attacks, LTD, LIDAR, and LRF systems operate independently of any optical receiver the target may have. Because of this, an adversary can choose the wavelength and other parameters of the threat laser.

Traditionally, laser rangefinders emit short pulses on the order of 10 ns at low repetition rates around 10 Hz [6]. LRFs and LTDs are typically based on Nd:YAG lasers operating at 1.06 µm wavelength [4] [5]. Laser target designators and LIDAR units also use short modulated pulses, around 10 ns [5]. The modulation encodes the transmitted signal reducing the risk of spoofing or jamming risks as well as interference [5].

Ground Based Systems

The background noise due to solar and stellar irradiance is reduced at longer wavelengths, motivating the use of CO2 lasers, operating in the mid-infrared or far-infrared wavelengths, for ranging applications [6]. However, the 9 µm to 12 µm wavelengths emitted by a CO2 lasers are highly absorbed by water vapour and as a result, the effectiveness of a ground based CO2 laser would be strongly limited based on cloud coverage and humidity [7]. Because of this it is common for military rangefinders to be based on 1.06 µm Nd:YAG lasers or 1.55 µm Raman Shifted Nd:YAG lasers [4] [8]. However, this limitation would be lifted for a satellite-to-satellite sensing or targeting devices.

Orbit Based Systems

For decades laser-based sensing and targeting technologies have been developed for, and used in, space. Adversarial spaceborne laser-based sensing and targeting systems will likely be akin to theses preexisting technologies. One such example is NASA’s lunar orbiter laser altimeter (LOLA), which operates at 1064.4 nm, 28 Hz pulse [8].

In general, pulsed lasers operating at wavelengths of 1064 nm or around 1550 nm are commonly used for spaceborne laser scanning systems. Older and long-range systems tend to be simple rangefinders, while newer and/or short-range systems tend to be used for LIDAR and/ or highly accurate measurements.

Dazzling, Jamming, and Spoofing

Dazzling, jamming, and spoofing are very similar ASAT attack vectors. They each target the satellites sensors with the intention of disrupting their proper functionality. China has carried out several satellite blinding activities to date [9]. Furthermore, there have been hundreds of recorded satellite jamming incidents by multiple different nation states and organizations as of 2011, and the relevance of dazzling, jamming, and spoofing has further increased since [2] [9].

It is possible to dazzle an Earth-observing satellite using a laser with only 1 mW of power, equivalent to that of a laser pointer, indicating the simplicity of such attacks [10]. The successfulness of such attack, as with any dazzling, jamming, or spoofing attack, is highly dependent on the target satellite’s detector assembly and corresponding optics. Various tests in the United States have indicated that lasers of hundreds or even tens of watts can temporarily interfere with military observational satellites [11]. Such laser with powers up to 10 W even have the potential to damage and destroy sensors [12].

Threat Summary

A destructive laser weapon is likely to be ground based due to the massive power requirements for such a high-powered laser, and the emitted beam is likely to be in the IR regime. Furthermore, a destructive ground based laser weapon would be limited in its effective range, only being able to affect satellites in LEO and potentially MEO.

Other non-destructive attacks are likely to originate from ground stations as well as space-based platforms at any orbit. Based on current military and civilian technologies, it is expected that these systems will operate using wavelengths in the visible through to the near IR regimes. The range and effectiveness of space-based non-destructive attacks would be limited by the size and weight restrictions of the platform hosting it.

4. OPERATIONAL ENVIRONMENT

It is challenging (though not impossible) for a satellite to remain in the FOV of ground-facing optical communication satellite due to the very narrow FOV. For example, a threat satellite orbiting below a target geostationary satellite with a FOV of 10 µrad, will only remain in the FOV for a maximum of 0.1 seconds assuming it does not maneuver. This is independent of the satellites' relative orbital altitude separation. For larger fields of view, the time spent in the FOV is significantly increased without any required maneuvering as shown in Figure 1 concerning LEO assets.

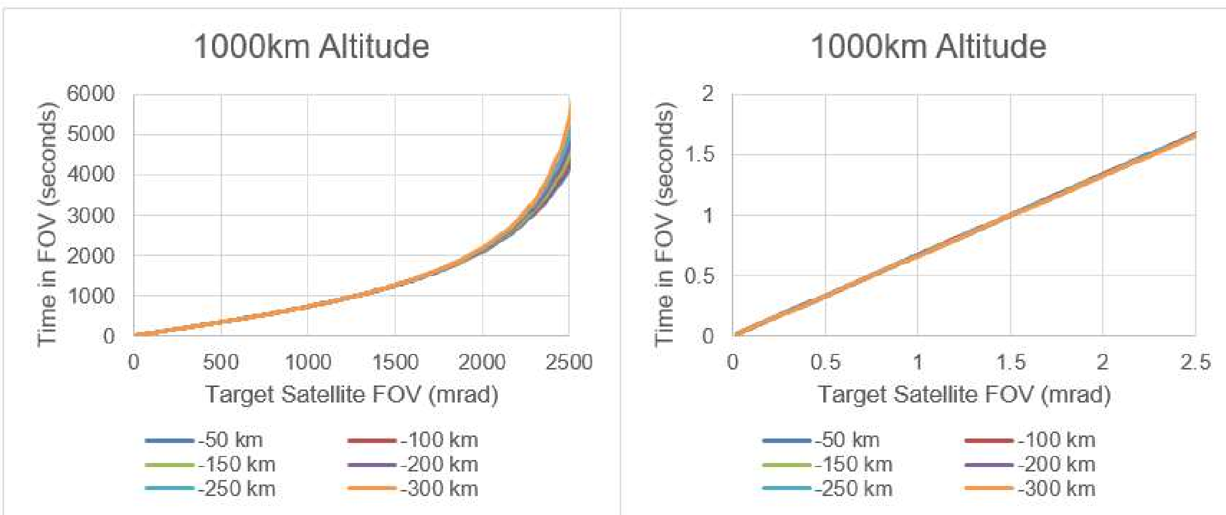

Figure 1 Time Spent in the FOV of a LEO Earth Observing Satellite
For a threat satellite orbiting below it without manouvering (1000km case). The different lines plotted corespond to the relative altitude difference in kilometers between the threat satellite and the target satellite.

Due to the vast number of different non-earth-facing observation orientations and potential co-orbital trajectories, only earth-facing observational examples were calculated. Additionally, it is more likely for an observational or communication satellite to be earth-facing than any other orientation.

Orbit based Systems

A threat satellite is only required to orbit beneath the target satellite if it intends to dazzle, jam, or spoof Earth-pointing sensors on the target satellite. This would be the case for ground to satellite communication or earth observation satellites. In other ASAT scenarios, such as laser-based sensing, targeting, or high-powered weapon attacks, the threat satellite, or ground station for that matter, does not require access to the target's sensor FOVs. The threat source could potentially share the same orbital altitude with the target satellite. As a result, their relative distances and speeds would be easily maintained due to the orbit similarity.

Ground Based Systems

For ground station based attacks, the distance to target and relative angular speeds would be very different than for a satellite-to-satellite attack. For a target satellite orbiting at low altitudes, there will be a high relative angular speed between the ground station and satellite. Inversely, for high altitude orbits such as GEO, the relative angular speed would be low, but the separation distance would inherently be higher. The relative angular speeds are also strongly depend on the orbit path as well as ground station location, so it is not feasible to accurately predict these features in a general sense. Figure 2 is presented as an illustration of the relative angular speed versus distance relation for a satellite and ground station rotating about Earth along the same plane and in the same direction. It is given as an example of one potential satellite and ground station configuration.

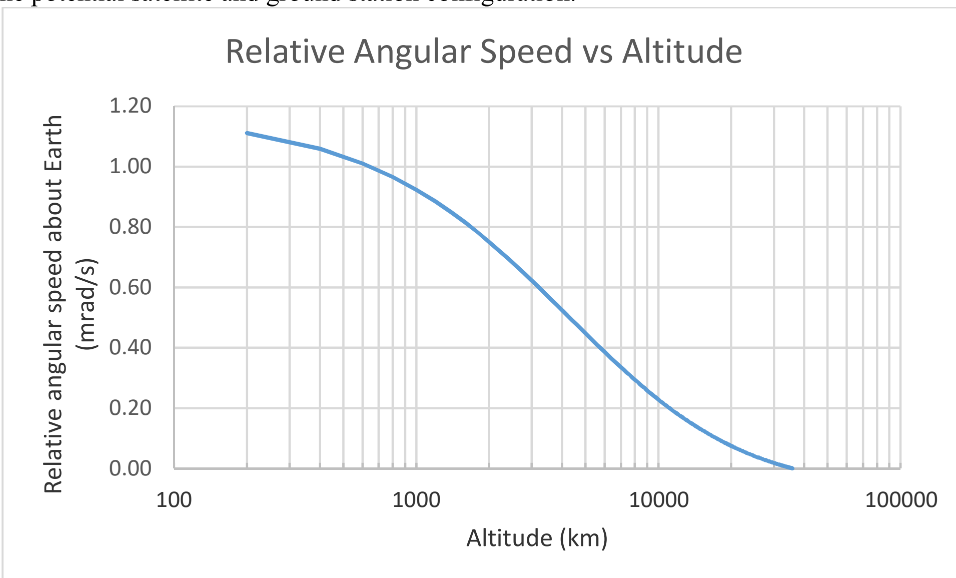

Figure 2 Relative Angular Speed About Earth's Equator Between a Satellite and Ground Station . Both are rotating along the same plane with respect to earth's centre.

5. SYSTEM REQUIREMENTS

Based on the assessment presented above, optical system requirements were derived for a baseline system as follows:

Table 2 Optical System Requirements

Requirement	Minimum	Ideal
Field of View	130 degrees	155+ degrees
Angular Resolution	0.5 degrees	0.1 degrees
Wavelength Bands	510 – 532 nm, 800 – 880 nm, 1058 – 1076 nm, 1540 nm – 1570 nm	450 – 485 nm, 500 – 565 nm, 625 – 740 nm, 800 – 880 nm, 1058 – 1076 nm, 1540 nm – 1570 nm, 2.7 and 3.8 µm, 9 µm - 12 µm
Laser Pulse Duration Detectable	< 1 nanoseconds	< 100 picoseconds

The minimum 130° FOV requirement is based on a, Earth-pointing satellite having an altitude of 500 km or higher. It also assumes a maximum viable ground viewing elevation angle of 10° due to atmospheric turbulence and scattering.

The ideal 155° FOV range is based the FOV required for an Earth-observing satellite positioned at the lower edge of LEO with an altitude of 160 km to view all of Earth. This would allow the system to locate any possible Earth-based threat.

An angular resolution of 0.5 degrees equates to a region with a diameter of less than 2 km at a distance of 200 km. This threat localization accuracy is expected to be sufficient for potential long-range satellite-to-satellite scan based on available technologies as presented in Table 1. The improved angular resolution of 0.1 degrees corresponds to a region with a diameter of less than 2 km at a range of 1000 km, which is representative of ground-to-satellite scans.

The minimum wavelength requirements given in

Table 2 are based on the wavelengths commonly used for military and space-based ranging, targeting, and communication activities as discussed in Table 1. The ideal requirements expands on the minimum requirements by including the 2.7 and 3.8 µm and 9 µm - 12 µm bands to cover wavelengths that may be used by long-range LRF, LTD, or LIDAR systems or even high-energy lasers. Wavelengths bands corresponding to red, green, and blue light are also added to cover the potential dazzling of cameras operating in the visible spectra.

The detectable laser pulse duration minimum requirement is on the order of nanoseconds as it is common to have pulse lengths on the nanoseconds scale for LRFs and LTDs. The ideal requirement of 100 ps detectable pulses is based on pulse lengths used by more complex LRFs.

6. BREADBOARD SYSTEM

A simplistic version (breadboard) of the flight system was assembled using COTS components. An image of the system under test is provided below.

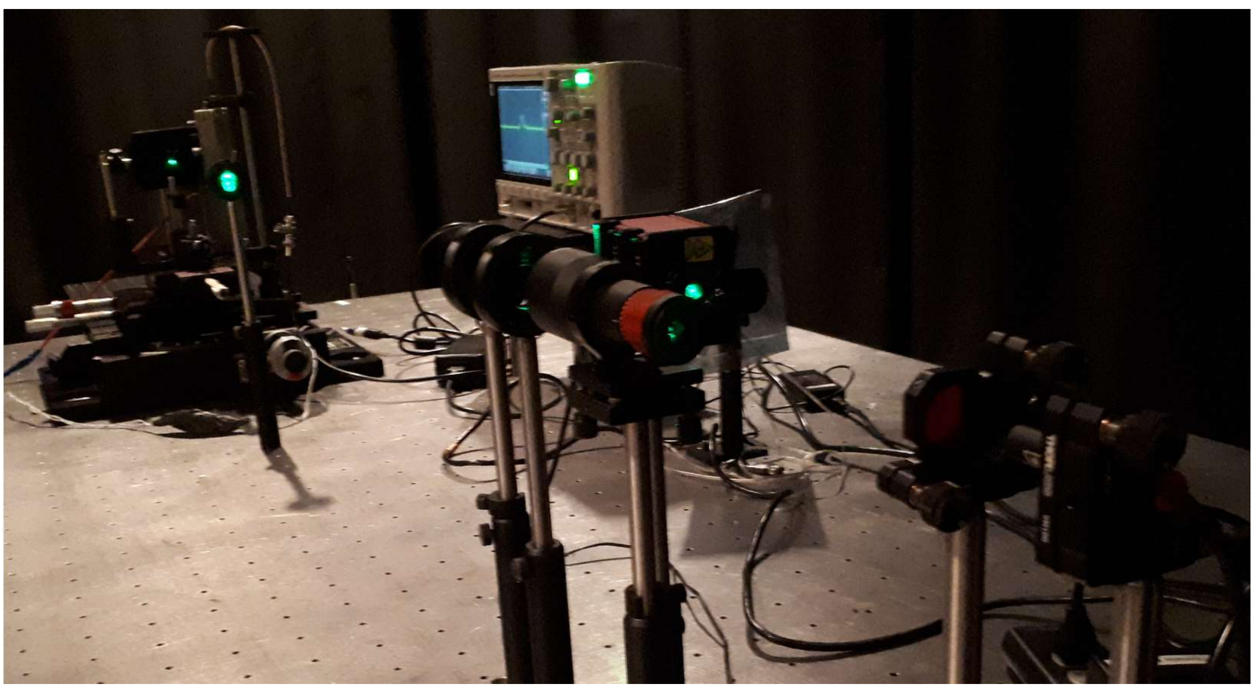

Figure 3 Breadboard Lab Setup

Results of breadboard testing indicated that specifications of the future flight versions of DOLOS are feasible as follows:

Table 3 Expected System Performance

Requirement	Expected Performance
Field of View	130+ degrees
Angular Resolution	0.1 degrees
Wavelength Bands	500 – 565 nm, 625 – 740 nm, 800 – 880 nm, 1058 – 1076 nm, 1540 nm – 1570 nm (+ Remaining Wavelengths)
Laser Pulse Duration Detectable	< 100 picoseconds

In addition to the wavelengths selected in Table 3, an additional data channel of any residual wavelengths was added. Although this does not provide wavelength information, it would provide a means of both characterizing the laser and providing incident beam location/heading.

The search algorithm employed to provide source location of the incident beam is capable of providing locations of two or more incident beams originating from different locals. This feature could prove useful over territories with multiple tracking lidar systems. A plot of these results is presented in Figure 4.

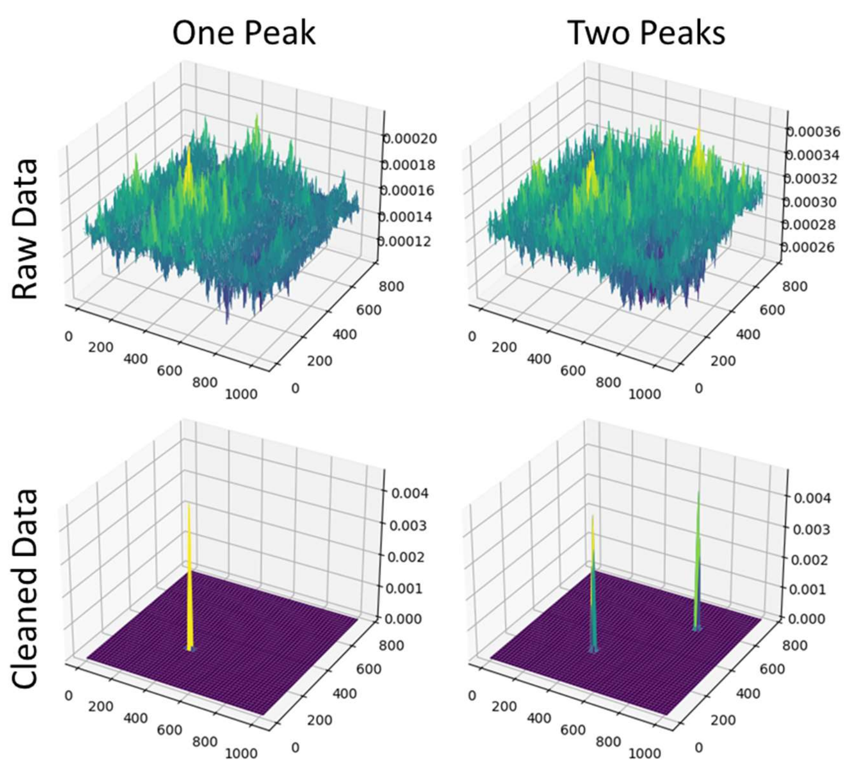

Figure 4 Localization of one or two incident beams.

Lastly, as assessment of components required to meet the space environment indicated that they represented a low risk to development. Next steps include incorporating a custom lens design to optimize signal detection limits, as well as creating a ruggedized version for use outside of the laboratory.

7. OPERATIONAL SCENARIOS

Error! Reference source not found.

The system will wait until an incoming signal is registered. In this mode, each detection of any signal will send the following information as a packet to the spacecraft (for transmission to ground):

- Detected wavelength
- A profile of the incident pulse
- Time of pulse detection
- Spacecraft ephemeris
- Position within the FOV (This will vary depending on passive or active mode)

The system will remain in the passive observational mode where all the light collected by the wide-angle lens is allowed through to the detectors, observing the entire FOV. This will continue until the detection of a pre-set number of pulses have been detected (to be determined during prototyping) – essentially after the laser characteristics have been established.

Once laser characteristics have been established, the system will be triggered to switch to Active Mode to attempt to determine the direction of incident light.

Active Monitoring Mode

Here the heading of the incident laser is determined to within 0.1°. Based on breadboard testing, it would be able to localize a threat 450 times a second. This localization frequency satisfies the 1 Hz imaging rate recommendation mentioned in Section 4.

8. CONCLUSIONS

A breadboard of the Detection Of Laser Operations in Space (DOLOS) system was developed and showed the feasibility of a laser threat detection system for space borne assets. The system will detect, characterize, and localize incident laser pulses. This allows for determination of both the type of system, and more importantly, the direction from which is was initiated.

9. REFERENCES

[1] D. Jacques. Very High Angular Resolution Laser Beam Rider Detector Having a Gated Image Intensifier and a Video Camera US PTO 5,280,167

[2] Defense Intelligence Agency, “Challenges to Security In Space,” 2019.

[3] T. Harrison, K. Johnson, T. G. Roberts, T. Way, M. Young and M. C. Faga, “Space Threat Assessment 2020,” Center for Strategic & International Studies, 2020.

[4] H. Kaushal and G. Kaddoum, “Applications of lasers for tactical military operations,” IEEE Access, vol. 5, pp. 20736-20753, 2017.

[5] M. E. Rogers, “Lasers in Space Technological Options for Enhancing US Military Capabilities,” Air War College, Maxwell Air Force Base, Alabama, 1997.

[6] R. Opromolla, M. Grassi, G. Rufino, G. Fasano and L. De Luca, “Advanced LIDAR-based techniques for autonomous navigation of spaceborne and airborne platforms,” University of Naples Federico II, 2016.

[7] L. Lyubomir and E. Teirumnieks, “Applcation of Laser Technology in the Army,” in International Scientific Conference “Defense Technologies", 2018.

[8] V. Molebny, P. F. McManamon, O. Steinvall, T. Kobayashi and W. Chen, “Laser radar: historical prospective—from the East to the West,” Optical Engineering, vol. 56, no. 3, 2016.

[9] T. Dekel and R. Levi, “Space Security Capabilities and Trends,” in Space Security Conference, 2011.

[10] D. Wright, L. Grego and L. Gronlund, “The physics of space security,” American Academy of Arts and Sciences, 2005.

[11] M. P. Pillsbury, “An Assessment of China's Anti-Satellite and Space Warfare Programs, Policies and Doctrines,” US China Economic and Security Review Commission, Washington DC, 2008.

[12] U. Tatar, A. Gheorghe and O. Keskin, Space Infrastructures: From Risk to Resilience Governance, IOS Press, 2020.