

The Mechanics of Spaceborne Warfare

INTEGRATING STEALTH TECHNOLOGY IN ORBITAL ASSETS

(Part of the Nightshade Advanced Polymorphic Defense and Warfare Doctrine)

By
Adib Enayati, Ph.D.

Cyber/Electronic Operations and Warfare



The Mechanics of Spaceborne Warfare: Integrating Stealth Technology in Orbital Assets

Adib Enayati, Ph.D.
Cyber/Electronic Operations and Warfare

Table of Contents

1. Disclaimer
 2. Document Identifier
 3. Dedication
- **Introduction**
 - **The Principles of Spaceborne Warfare**
 - *Precision*
 - *Guarantee*
 - *Continuity*
 - *Consistency*
 - *Interoperability*
 - *Integration*
 - *M2 Factor*
 - *Protection*
 - *Independent Balanced Access*
 - **Orbital Suppression principle**
 - *STAP (Smart Target Acquisition Protocol)*
 - *DHS (Direct Harmonized Suppression)*
 - *MOTC (Maneuverable Orbital Targeting Components)*
 - *AID (Adaptive Integration and Development)*
 - **Stealth in the Concept of Force Protection**
 - **Understanding Stealth Technology**
 - *Primary Design Concepts (Passive)*
 - *Secondary Design Add-ons (Passive)*
 - *Active Stealth Components*
 - **The Concept of Stealth in Spaceborne Warfare**
 - **Satellite Detection, Identification and Tracking**
 - *Terrestrial Based Radar Tracking*
 - *Optical Tracking*
 - *Hybrid Tracking and Signal Mapping*
 - *Radio and Communication Tracking*
 - *Space Based Sensory Detectors*
 - *Suborbital Detection*
 - *MASINT, SIGINT, ELINT, CYBER and Intelligence Operatives*
 - **Understanding the Detection and Tracking Methodology**
 - **Incorporating Stealth into Spaceborne Assets Design and Development**
 - **Introducing Spaceborne Mission Control Hubs (SMCH)**
 - **Adapting the Use of Active Spaceborne Decoys**
 - **References**

DISCLAIMER

The contents of this paper are exclusively formulated by the author and do not reflect or utilize the views or data from any United States government entity, agency, or institution. The objective of this paper is to present the fundamental concepts, limitations, and factual insights pertaining to its title and the associated subject matter. It is important to clarify that the author has no affiliation with any governmental military or intelligence agency. Therefore, any attribution of the author's work to such entities is unfounded and without merit.

DOCUMENT IDENTIFIER



SERIAL NO / P00-9955840047



MAY 30 2024 / AUUTHC 9892-B



MAY 30 2024 / RELTO P00



//RELTO/P00

Copyright© and Author's Notice

Author: Adib Enayati, Ph.D. —Cyber/Electronic Operations and Warfare

Publisher: The author has decided to publish this paper publicly due to lack of specialized journals for this subject and their length, distribution and access limitations and to eliminate the copyright claims of the third-party publishers that would impose restrictions on the republication and redistribution of this paper. This paper is published openly for maximum access and availability.

Date of Publishing: 05/30/2024—00:00 EST



Notice:

An official written permission is required for redistribution of this paper and its content from the author for the purpose of the republication and redistribution. Otherwise, you are free to use the content of this paper for your defense planning and success. After all this paper was intended to enhance the specific (Defense Industrial Base) and public sector's capabilities to protect themselves in the face of the modern threats and ultimately to be able to advance the interest of the United States of America. Use of the third-party logos, such as the publisher's logo is permitted only with a written permission from the publisher and the author has no authorization in granting such permission to anyone. You are not authorized to attribute this paper to any United States government organization or entity and you are bearing full responsibility for falsifying such attributions and the unlawful use of their trademarks, logos and insignia should such a case occur. Should you have any questions and requests regarding this paper or you simply wish to contact the author, feel free to reach the author via this email: adibenayati.public@outlook.com. This entire paper is the work of the author alone. There are no citations, reference and remarks from any third parties due to the fact nothing of this paper has been taken from any third-party sources. Any commercial use of the ideas presented in this paper for developing any software or hardware is strictly subjected to the author's permission. The author's seal represents the office of the author and it shall not be attributed to any third-party entity. This notice is in effect as of May 30, 2024, 00:00 Zulu time.

To the brave men and women who serve and protect the United States' interests in the vast expanse of space, your unwavering dedication, pioneering spirit, and relentless pursuit of excellence inspire us to push the boundaries of innovation and technology.

May this work contribute to the advancement of your mission and the continued security and superiority of the United States' space capabilities.

Introduction

As we delved into the role of satellites in the previous paper, titled “The Mechanics of Spaceborne Warfare: Exploring Anti-Satellite Operations,” we established the indispensable role of satellites in today’s military networks and how the Space-based ISR assets are crucial for any modern military networks. Satellites play roles from ISR (Intelligence, Surveillance, and Reconnaissance) to communications and strategic navigation, which enable the guidance and precision of many of the United States arsenal. We also discussed the role of satellites in enabling many disciplines of Intelligence such as MASINT (Measurements and Signatures Intelligence), ELINT (Electronic Intelligence), SIGINT (Signals Intelligence), IMINT (Imagery Intelligence), GEOINT (Geospatial Intelligence), and FISINT (Foreign Instrumentation Signals Intelligence).

Anti-satellite operations and warfare are a vast subject that has not really changed much since its conception, which is why I introduced the novel concept of orbital suppression in the paper titled, “The Mechanics of Spaceborne Warfare: Redefining Orbital Suppression Dynamics.” The concept of orbital suppression gave a new definition to anti-satellite operations and warfare, a concept with its own principles that changed our perception of modern spaceborne warfare. The principles that we have defined for spaceborne warfare gave a whole new practical understanding to the subject in discussion, and as I introduced its enhanced principles in orbital suppression, we outlined the future of spaceborne operations and warfare.

In this paper, I will be introducing the integration and incorporation of stealth technology into future spaceborne assets. However, before we can get there, we should cover a lot of ground and delve into the past,

as well as the concepts surrounding the introduction of stealth in satellite designs and spaceborne warfare.

My determination on ensuring the absolute superiority of the United States in space is very much the core driving factor for this paper, as I aim to lay the foundation for a new concept in satellite design. Much like any meaningful advancement in history, this is an interdisciplinary approach. You must have the knowledge of advanced aerospace engineering, as well as electronic warfare, radar design, material science, military science, intelligence, and cyber operations. The concept aims to encourage the design and development of several key components before one is able to design a “Stealth” satellite that can live up to its name and purpose. This subject requires further investment and development if we are to build the next generation of spaceborne assets with the objective of “Absolute Superiority of the United States” in sight.

First, we will dive into the spaceborne warfare principles for both anti-satellite operations and the novel concept of orbital suppression, and then move on to introducing stealth technology while understanding how adversarial detection works and finally painting the picture of the concept of stealth satellite design. I dare to deviate and introduce the novel concept of the use of Spaceborne Mission Control Hubs (SMCHs) and active spaceborne decoys in order to enrich the subject of spaceborne warfare at the end. Since this paper is a public release, I must refrain from expanding on some of the concepts that I introduce to maintain a veil of secrecy in the interest of national security. Therefore, I may not dive deep into some subjects and do a detailed How-to as I aim to introduce this concept in the favor of the United States and not its sworn adversaries.

I, once again, would like to emphasize the importance of the expansion of redundant

terrestrial capabilities to ensure the preservation of force-protection principle, and to ensure that the United States can maintain its strategic capabilities in any theater conditions as adversaries focus on the development of the capabilities to target the United States' spaceborne assets and capabilities. It is paramount to understand the adversarial aim and planning as well as monitoring their capabilities and capacities, and it is paramount to begin the development of the next generation spaceborne assets to maintain the technological gaps between the United States and its adversaries.

The Principles of Spaceborne Warfare

Much like any military operations; the core principles of war apply in any mission planning. However, the Spaceborne warfare has its own core principles. While the essence of the military operation is the same, the very nature of the space-borne operations and warfare demanded its own principles. I established the following core principles in "The mechanics of spaceborne warfare: Exploring Anti-Satellite Operations":

- **Precision:** Any kinetic and non-kinetic action has its own consequences. Precision implies the importance of targeting what we want while inflicting minimum unwanted damage to others. Precision is highly regarded in the modern electronic warfare because as we aim to target the adversarial capabilities, while safeguarding our own. So, precision while can be resource exhaustive, must be implemented unless the theater requires otherwise.
- **Guarantee:** The operation should guarantee to achieve the laid-out objectives. Regardless of what we do or the theater, the principles of war apply.

We have to manage our EOF (economy of force) while ensuring mission success as prescribed by the mission objectives.

- **Continuity:** The ability to target the adversarial capabilities must be continuous and the components of the mission must be able to operate with continuity. None-Kinetic options are extremely important as they have the potential for operational continuity yet they are dependent and limited by the energy factor. We must ensure the operational continuity in our designs and engagements. Managing the resources are extremely important in maintaining a steady combat capability.
- **Consistency:** The Components must be able to achieve results with consistency. This emphasizes the important of understanding the adversarial defensive capabilities in a continuous manner in order to be able to maintain the offensive capabilities.
- **Interoperability:** The abilities, hardware, weapon systems and human resources should be employable and operable by all branches of the armed forces. This will enhance the combat capacities across the armed forces spectrum and ensures mission success especially if regulated None-Kinetic options are authorized for wider use by all the components.
- **Integration:** The existing concepts, strategies, abilities, hardware and weapon systems must be integrated into all branches of the armed forces to maximize their combat readiness and protection.
- **M2 factor:** This refers to the Mass and Mixture, the weapon systems and the concepts used should have the power and the effective mixture to be combat

effective against the adversarial capabilities at all times. The redundancy in the offensive capabilities is extremely important.

- **Protection:** Regardless of what we do to achieve our combat objectives, one of our primary goals is force protection. Our operations, concepts and planning should consider the survival and continuity of the friendly capabilities at all times.
- **Independent Balanced Access:** As I have written about the concept of a resilient and redundant COC several times in the past, we should understand that the adversaries are aiming to achieve the same objectives as ours. While they might achieve some levels of success, all regional commands must have the ability to utilize the Anti-satellite warfare independently while being able to protect the friendly capabilities. This will enhance the survivability and combat effectiveness should the necessity arise. However, strong protocols should be in place and as we have already established, ensuring that the friendly and adversarial “strategic” protocols are not disrupted should be a fundamental principle.

Orbital Suppression is a new concept in spaceborne warfare. The concept would utilize hybrid technology rather than pure kinetic and non-kinetic methods to suppress the entire orbit in a tactical or strategic manner. This new modern approach, in contrast to the classical spaceborne warfare, presented a new range of options. The following Enhanced Principles in “The Mechanics of Spaceborne Warfare: Redefining Orbital Suppression Dynamics” have been introduced to support the concept and the future developments for the operations supported by this concept:

- **STAP (Smart Target Acquisition Protocol):** This core principle works based on the adversarial spaceborne command and control dynamics. Since we are still focusing on a geographical area opposed to the orbit itself, targeting the right area that can tactically contain the components of the adversarial C6ISR is the key. This would recommend the target area to be the Uplinks, Mission Control Centers, Command and Control Infrastructure and Fixed Strategic Missile Silos, Adversarial Communication Relays as well as mobile components which are enabling field tactical access to the existing strategic network. By digesting this principle, a target bank can be constructed based on the order of battle in any theater.
- **DHS (Direct Harmonized Suppression):** In the previous paper we have established that the adversaries have a special focus towards their terrestrial capabilities and capacities in the absence of superior spaceborne capabilities and as a redundant protocol. The success of the orbital suppression missions demands the kinetic and non-kinetic destruction or disruption of the adversarial terrestrial capabilities across the theater to ensure that full suppression can be achieved as the adversarial terrestrial capabilities are core components of their redundancy protocols, identifying and targeting the terrestrial capabilities via kinetic and non-kinetic means is essential to a successful orbital suppression mission. This will ensure the full termination of any redundant protocols in place. This, however, can

be achieved by tactical or strategic approaches.

- **MOTC (Maneuverable Orbital Targeting Components):** Mobility and developing mobile components are essential for strategic and tactical orbital suppression. Mobile capabilities guarantee maneuverability and therefore rapid deployment and redeployment as required by the theater. Maneuverability and sustainability are a very important factor when it comes to the design of military equipment. Mobile and self-sustainable systems are capable of conducting missions in an extended time and range and therefore support other principles of the warfare and spaceborne warfare.
- **AID (Adaptive Integration and Development):** Building Multipurpose weapon systems should be a standard protocol. The suppression weapon systems can be incorporated into the existing platform and can have a universal modular design concept. This cuts both ways, part for suppression and part to support the redundancy of the friendly capabilities to combat any form of adversarial suppression. This will ensure that the preservation of the friendly capacities at all times. This, however, demands great mobility.

As you might have noticed by reading the previous papers, the principle of “Force-Protection” is the fundamental principle in any spaceborne operation. The ability to preserve friendly capabilities while being able to disrupt adversarial capabilities remains a key focus and challenge, which is why I placed great emphasis on the enhancement of terrestrial and temporary

suborbital redundancies. The force protection concept has a far broader aim than just preserving friendly assets and capabilities. The emphasis is also on spaceborne asset survivability as much as the preservation of friendly capabilities, as both have a direct correlation with each other.

Stealth in the Concept of Force Protection

The current focus of this paper is the introduction of stealth technology for spaceborne assets. Incorporating stealth technology will enhance the survivability of spaceborne assets and therefore contribute to the principle of “Force Protection.” There are, however, serious challenges with regards to this concept that we will address as we introduce it.

It is also important to understand the stealth technology itself, which is why we will take a short time to introduce and digest it. Part of the reason that stealth has never been incorporated in space has a direct relationship with the needs and requirements for spaceborne assets. As adversaries have evolved and developed their arsenal to combat the United States’ spaceborne assets, the need for protection for these assets has increased rapidly.

We have covered the concepts of anti-satellite warfare thoroughly in the first paper (“The Mechanics of Spaceborne Warfare: Exploring Anti-Satellite Operations”) and we are not going to expand on them here. However, I would dare to say that applying the concept of stealth in an asset-specific manner would enhance asset survivability against kinetic and non-kinetic techniques. Take note that espionage and cyber operations and warfare still remain a challenge for the protection of spaceborne assets.

Understating Stealth Technology

I would define stealth as a mantra of active and passive techniques and technologies which enable assets to remain undetected by the detection assets of an adversary. Take note that stealth in any way does not mean invisible; the incorporation of stealth into an asset will only make it hard to detect, as adversarial assets in stealth detection are limited. The cost and complexity of the detection of stealth assets are high for the adversaries, and the United States' advancement in stealth technology has enabled it to produce great stealth assets which have become a focus for the adversaries.

I have mentioned that stealth has active and passive components. The passive components of stealth technology can be broken down into "Primary Design Concepts" and "Secondary Design Add-ons." We will break down these two shortly, and I try to simplify the concepts as much as possible.

Primary Design Concepts (PASSIVE):

As we are designing any airborne or spaceborne object, we start with the design of the physical features. The science behind stealth design is not so simple when it comes to cost effectiveness as well as the functionality of the designed platform. Understanding the interaction of radar and radio waves with the material to symmetrical design that will aid the dispersion or absorption of incoming radio waves and balancing the design with functionality and cost is the actual challenge. The stealth design would avoid right angles and cavities that can reflect or become the propagator of standing waves, which is why we usually put a lid on everything and try to cover everything within the airframe of the object. Further on, we have to create symmetry, which is nothing short of an art in design. As

I have been describing this, you probably were imagining the airframes of the superior F22-Raptor or the F35; Keeping the shape and concepts in mind for a fighter jet, the length and shape of wings and control surfaces are extremely important as well. If you notice, both jets have a cone shape contributing to lowering their RCS (Radar Cross Section). Their control surfaces are designed to avoid Rayleigh Scattering. A fighter jet requires evading a wide array of radar systems, which is why its design has to be balanced. Remember, Stealth does not mean invisible to radar; it is just harder to detect at certain frequencies and sometimes it is invisible to certain frequencies. However, as a fighter jet or a bomber has to remain undetected to a wide range of terrestrial and airborne assets, active stealth components are incorporated. Take note that as we aim to introduce several design components for spaceborne assets, it is paramount to understand that incorporating stealth into spaceborne assets will have far more implications on asset functionality and cost, not to mention the cost of deployment into orbit.

- ***Secondary Design Add-ons (PASSIVE):*** Passive design components alone are not going to create a fully functional stealth design. Once again, I would like to bring your attention towards the known stealth assets such as the F22-Raptor and the B2-Spirit. The secondary design add-ons involve coating and composite materials. The composite materials as carbon fiber reduce the RCS greatly especially if they are used for wings and control surfaces. The use of RAM (Radar Absorbing Materials) is an important part of the design add-ons. Take note that in a fighter jet; the main causes of standing waves are the engine

intakes and the canopy which is why the canopy has to be coated with special materials. The use of the composite materials will also greatly reduce the conductive surface area of the object (Utilizing Maxwell's Theory) to reduce the reflecting surfaces of the craft. Since the subject of this paper has a special focus on the satellites, we will not be dissecting the RAMs and the coating materials in depth; however, it is extremely important to understand that the RAMs and Coatings are very expensive and have a short lifespan which is why the stealth jets usually "Shed Skin" after a while and therefore maintenance is required to reapply the coating on the surface of the planes. While so, we will not be having the luxury of doing the same kind of maintenance for the spaceborne assets. It is impractical to use traditional RAMs and Coatings for the spaceborne assets. Take note applying traditional RAMs and Coatings to any spaceborne assets will increase the weight of the asset greatly and therefore increasing the cost of the deployment of the asset as well as shortening its lifecycle. Furthermore, we will not do the subject justice if we ignore the optical stealth component of camouflage for terrain masquerading.

As we briefly delved into the passive components of the stealth mantra, we now understand the challenges surrounding the integration of stealth technology in spaceborne assets. However, these challenges are relatively easy to overcome with the integration of active stealth components into the design. At the end of the day, we have to balance the design and the cost. Space missions are not cheap; while we have made great advancements in making

the cost of space missions more balanced and cheaper, every mission comes at great logistical costs. Additive manufacturing plays a vital role in keeping space missions cost-effective, but the design and development of a space asset are still high.

- **Active Stealth Components:**

Active stealth components are a work of art. The DRFM (Digital Radiofrequency Memory) technology has enabled manufacturers to produce a wide range of countermeasures as well as active stealth components. You need to have a basic understanding of radar systems as well as the principles of interference to comprehend this small subject. Radar is short for Radio Detection and Ranging. It propagates radio waves to the target and analyzes the reflected signal. Unlike sound, radio waves are what we call transverse waves. While sound requires a medium (AIR), transverse waves (e.g., radio waves) do not require a medium, and they can travel at the speed of light in the atmosphere, which makes them suitable for radar applications. However, the frequency of the radar and its interaction with the Earth's atmosphere is an in-depth concept of its own, which has led to the development of OTH (Over the Horizon) and Space Monitoring Radars. There are many concepts that enable a radar system to become what it is. The radar pulse, signal processing, and Doppler frequency mechanics are basic concepts that enable the development of advanced radar systems. Since we are not in a radar design course, we will not be diving into those concepts. If you are familiar with the principles of wave

interference, you would understand that radio waves (and all forms of waves, even sound waves) follow this. The active components are capable of recording the incoming radar pulses and generating canceling waves, which will in effect cancel or disrupt the incoming radar pulse in order to prohibit the transmission of the radar pulse from the plane, and therefore blend in with the noise floor below the radar detection threshold (also known as the Signal to Noise Ratio of the radar system). This can be done to the search and detection radars as well as targeting and firing solution radar systems. There are several active components that grant the stealth plane the ultimate capability to avoid radar detection. Remember, stealth does not mean invisible and doesn't grant invincibility to an asset.

Aside from the DRFM, which is the foundation of modern stealth, this category involves active cancellation devices designed to emit canceling waves to create interference with radar signals, Electromagnetic Cloaking Techniques involving the use of materials that can essentially bend electromagnetic waves around an object and make it undetectable to certain frequencies, plasma stealth, and ultimately adaptive radar absorption materials. These are comprehensive topics in active stealth technology and have practical applications in this paper. However, due to the sensitivity of the subject, I refrain from expanding on these subjects further.

By now, we have delved into the concept of stealth, and as you understand, it is a complex yet easy-to-navigate concept. Stealth design is a force multiplier that can increase asset survivability and greatly

contribute to mission success. Combining stealth technology will make spaceborne assets harder to detect and track by adversaries, therefore directly contributing to the force protection principle and protecting the assets. In the next section, we are going to dive into satellite detection, identification, and tracking, as understanding these concepts is crucial for any individual who is planning to incorporate stealth design into future platforms. Stealth can be interpreted as a form of hardening the assets as well.

The Concept of Stealth in Spaceborne Warfare

Incorporating stealth into spaceborne asset design can introduce a whole new concept of the fog of war in spaceborne warfare. The stealth concepts will also help protect these critical assets and their missions. I have always prioritized the absolute superiority of the United States in the final frontier above all considerations. However, this does not mean blind deployment and development of space-borne assets. If we break down the spaceborne assets, I would categorize them into two categories:

- ISR/Communication Assets
- Weaponized Assets

Both series of assets must be present to contribute to United States supremacy in space, and one cannot exist without the protection of the other. Stealth design is needed to protect both categories of assets with different configurations. Perhaps maintaining the fog of war, itself is a contributing factor to force protection. Adversaries should work hard to gather intelligence with the lowest rate of success. Spaceborne assets are the backbone of any modern military networks, and defending them is becoming more complicated every day. By introducing stealth into the design of space-borne assets, we might increase costs,

but we create the new generation of spaceborne assets. This is not just about passive and active stealth components. The concept itself, as we will explore, addresses far more complex concepts for the creation and protection of next-generation space assets that can guarantee the fog of war remains in the favor of the United States and keeps stretching the technological gap between the United States and its adversaries. It is now about balancing costs and lifecycles with individual asset superiority, which is a contributing factor to overall dominance in space.

Furthermore, we need to consider the use of stealth in single assets or asset constellations. While I encourage the use of the stealth concept, I suggest this concept remain asset specific until the full design and development lifecycle are researched and developed. This is a major leap in satellite design, and when such a major leap is discussed in the development of critical strategic assets, caution is often advised to avoid unwanted complications or mishaps. The stealth technology itself is well known and researched, but the integration of the technology must be balanced with operational and logistical limitations.

I believe that this concept defines the future of satellite design. I believe that this concept, much like orbital suppression, will usher in a new era of spaceborne warfare as we muster and master our capabilities, and I am confident that the United States will pioneer this development as it always has.

Satellite Detection, Identification and Tracking

While we are discussing the concept of stealth in spaceborne assets, one must understand the limitations of spaceborne asset detection. Detection of spaceborne assets starts from the moment of the preplanned launch of the asset. As we have

established in the previous papers, tracking adversarial satellite launches is an important factor in enabling the establishment of a robust detection strategy. Unlike civilian satellites, military satellites do not announce their identification and position publicly for tracking. As satellites are the backbone of United States strategic capabilities, it is only fair to assume that adversaries are carefully observing and tracking every mission launch in the United States. However, the concept of satellite detection consists of:

- ***Terrestrial Based Radar Tracking:*** Ground-based radar systems are designed to track high-altitude objects following specific patterns. We know that for a vector to break orbit, there are specific requirements, and each stage can be monitored via ground-based radar tracking stations. Do not get confused; there are many radar systems designed to cover high altitudes and azimuths. These radars usually operate in UHF (300 MHz to 3 GHz), L-Band (1 GHz to 2 GHz), S-Band (2 GHz to 4 GHz), C-Band (4 GHz to 8 GHz), X-band (8 GHz to 12 GHz), Ku (12 GHz to 18 GHz), and Ka (26.5 GHz to 40 GHz) bands. The tracking detection varies as the resolution of the radar has a direct correlation with the frequency it operates in. The UHF band is usually used to detect objects, whereas higher bands are used for accurate tracking due to the higher resolution they offer. You must assume that tracking is being done with all the resources available to adversaries and identify all adversarial tracking assets.

- **Optical Tracking:** There are telescopes dedicated to acquiring visuals from spaceborne assets. The optical tracking assets are designed to track and capture footage and photos of satellites as they pass over a geographical area. This will aid in the identification of satellites in orbit, and it will help classify their capabilities.

- **Hybrid Tracking—Signal Mapping and Observations:** The use of multiple sensory systems in real-time is called hybrid tracking. Special sensors that are able to detect spectrum-specific communications can be deployed to detect any form of communications from unknown objects (e.g., Nightshade’s Odin Electro-Optical Sensor). The concept of hybrid tracking can have different definitions in different disciplines, but as I focus on passive and active detection of spaceborne assets, it is important to understand the concept in the context of this paper in order to avoid confusion. Signal mapping is another technique that can aid in the detection of satellites by mapping and categorizing all known signals with their corresponding modulations used by spaceborne assets and their terrestrial mission controls.

- **Radio and Communication Tracking:** Every satellite has to communicate with its mission control; military assets are no different from civilians’. Every satellite or class of satellites has to communicate on a certain frequency. This involves two-way communication from the satellite’s downlink and terrestrial mission

control’s uplink. Monitoring of space and terrestrial assets and correlating the data can provide valuable information for the identification and classification of spaceborne assets. These communications can be intercepted, as satellite communication is still a wireless broadcast.

- **Space-based Sensory Detectors:** The space-based sensory detectors are satellites placed in higher orbits and are dedicated to observing and monitoring the lower orbits for any satellite activities. They play a vital role in tracking satellites in the lower orbits. These sensory systems are also capable of monitoring satellite launches and pinpointing their launch positions, tracking the vector to its destination with predictive algorithms.
- **Suborbital Detectors:** High-altitude missions are used to detect spaceborne assets in different geographical regions where detection methods are less accurate or available. High-altitude balloons or aircraft can collect ELINT and photography from orbital assets for further processing.
- **MASINT, SIGINT, ELINT, Cyber and Intelligence Operatives:** Perhaps the most comprehensive discipline of intelligence gathering and analysis mastered by the United States is MASINT (Measurement and Signatures Intelligence), capable of tracking and tracing the smallest signatures using a wide range of superior spaceborne and terrestrial-based sensory networks. The United States’ adversaries, such as Russia and China, have made progress in expanding their sensory networks to

support their MASINT endeavors. ELINT (Electronics Intelligence) and SIGINT (Signals Intelligence) are also crucial disciplines in intelligence and satellite detection. It is important to note that the classification of satellites, identification of their systems and subsystems, as well as their uplinks and downlinks, all fall under SIGINT and ELINT, not to mention traditional espionage to access designs and other important data surrounding an orbital asset. Accessing classified or even controlled classified information by intelligence operatives or cyber operations can provide invaluable insights regarding spaceborne assets.

Take note that some satellites are able to determine their own accurate position via GNSS and send the information via downlink to their mission control, which can be intercepted and decoded.

Understanding the Detection and Tracking Methodology

If we break down the tracking methodology, the first step involves space-based sensory detectors detecting and tracking any launches (excluding espionage). As these systems track the vector to its intended destination, terrestrial-based radar tracking assets can focus on scanning the orbit to detect the new object and determine its speed, position, and orbit to plot an orbit for the tracked object. The third phase is to acquire a visual of the object to identify and classify it. The fourth phase involves determining its telemetry frequency, as well as downlink and uplink frequencies, to feed ELINT (Electronic Intelligence) for future anti-satellite or orbital suppression operations planning.

Unlike airborne objects that can change trajectory, speed, and altitude at will,

satellites are static objects and must follow orbital dynamics. While a fighter jet can change trajectory, speed, and altitude to utilize surrounding natural terrain for concealment, a satellite does not have this luxury. Once a satellite is placed into orbit, it must maintain a constant velocity to remain in orbit, exposing important characteristics like altitude, velocity, and direction to adversaries. This information is sufficient to plot a course and predict the object's exact arrival, aiding adversaries in developing Doppler-based models for accurate detection and tracking of spaceborne assets.

After a satellite is detected, the process of collecting ELINT (Electronic Intelligence), SIGINT (Signals Intelligence), and FISINT (Foreign Instrumentation Signals Intelligence) begins. The collected data can be recorded for further processing, where it will be used to classify the satellite, decode its transmissions, and set for continuous monitoring and tracking. This information is crucial for electronic and cyber-attacks against the asset and its mission control. This standard operating procedure for handling exposed adversarial orbital assets involves continuous effort in electronic and signals data collection.

Incorporating Stealth Into Spaceborne Assets Design and Development

Take a moment to digest the previous section. It is apparent that in order to avoid being tracked, we need to evade detection or make it very difficult, time-consuming, and resource-intensive for adversaries. This will inherently degrade their capabilities because they will have to expend significant time and resources to track and identify objects. Unlike airplanes, satellites do not have engines for maneuvering or much room for maneuvering, so stealth must be incorporated at the drawing board while

accounting for expensive redundant systems and systems that ultimately bring the satellite to life. It is crucial to maintain a cost-effective design to avoid going over budget or, worse, building something heavy that costs a lot to deploy. Those who have designed any component for the military understand that everything must be cost-effective yet meet rigorous standards. Adding stealth to the mix is going to complicate things, and since we rarely have an unlimited budget, we have to design smart. The key is understanding the asset's purpose and importance in the broad concept of spaceborne warfare. Different levels of stealth design can be incorporated based on the asset's role.

We know that the detection of an object by radar or optical means has a direct correlation with the shape, size, material composition, and characteristics of the object. Perhaps the most common defining factor for satellites are the large solar panels used to power the satellite subsystems. Utilizing RTGs (Radioisotope Thermoelectric Generators) together with advancements in battery and capacitor technology can contribute to eliminating the use of large solar panels, thereby reducing a significant contributor to the satellite's RCS. (Note that MASINT becomes more relevant in detecting such configurations.) The power source is the most critical component of the satellite, as it should provide uninterrupted power for the satellite's entire lifecycle. While RTGs do not contain high levels of fissile material capable of achieving critical mass, they are extremely toxic, and the risk of spreading radioactive materials on Earth is higher if they crash into the Earth's atmosphere during launch or prematurely prior to the end of service. If we assume that we develop a suitable and safe RTG for satellites, we risk increasing the weight of the power source and therefore negatively impacting satellite design as it will increase the mission's cost.

One could potentially design compact and retractable panels or sails for the satellite to address this factor; however, it is important to understand that more moving parts mean more unpredictable errors, and as we know, we do not have the luxury of satellite repair. As the most fundamental stealth design principle suggests, everything must be covered to avoid cavities that contribute to the generation of standing waves. Satellites have several communication antennas with different configurations, ranging from dishes to helical or monopole antennas; therefore, designing storage and cavities with proper covers is necessary for them. While this introduces more moving parts into satellite design, it can protect communication and telemetry components.

As we have established, satellites are static objects orbiting Earth in predetermined orbits with known velocities. There are several components that can help satellites become less visible. Understanding that stealth design dictates covering cavities with a lid or cover, this concept can be applied based on the type and classification of the satellite. It is important to note that the detectability of an object is determined by its shape, size, composition, and surface characteristics. Taking the sphere as an example, a spherical object tends to scatter radio waves more uniformly in all directions compared to flat edges, so let us assume spherical shapes in the frame design in this context.

I chose the spherical shape to demonstrate the concept, but before we delve into that, I want to point out the advantages and disadvantages of such a shape in satellite design. A sphere has perfect geometry, making it easy to design and manufacture. Spheres also offer structural integrity, as the load is distributed evenly, providing resistance to stress. Additionally, its minimal air resistance makes it suitable for satellites in Low Earth Orbit (LEO), where

atmospheric drag is a concern. Lastly, if the antenna is incorporated into its frame, it can accommodate antennas with omnidirectional coverage.

However, this design is not without disadvantages and trade-offs. You cannot incorporate many components inside the sphere due to the volume efficiency of the structure, assuming that we are not going to use solar panels in our design (opting for RTGs instead). Additionally, the spherical design may pose challenges to the deployment mechanisms of the vector during launch. Overall, please consider this as an example only.

Below, we plot the Radar Cross Section (RCS) of a simple sphere for comparison. The first plot shows the RCS of a sphere with a diameter of four meters across frequencies ranging from 300 MHz to 40 GHz. The second plot depicts the same sphere in Low Earth Orbit (LEO).

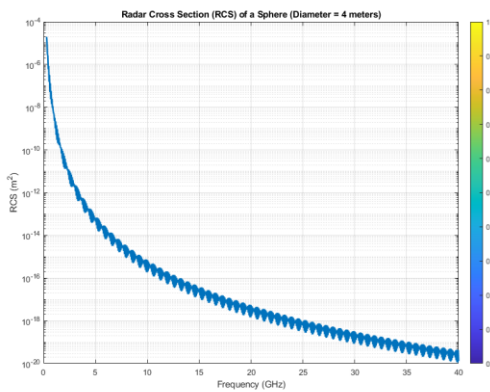


Figure 1 Radar Cross Section (RCS) of a Sphere with a 4-meter diameter

Take note that these plots are only a demonstration of the potential use of the spherical design.

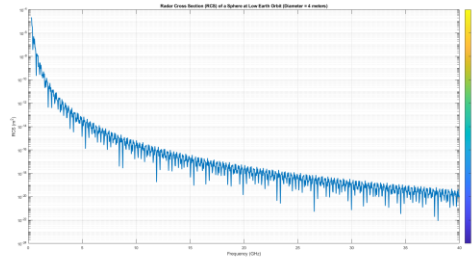


Figure 2 Radar Cross Section of a Sphere at LEO (2000 km) with four meters Diameter

To determine the actual Radar Cross Section (RCS), various factors must be considered, including the composition of the materials covering the sphere's surface, its shape, surface roughness, orientation concerning the observer, and environmental conditions such as atmospheric effects and electromagnetic interference. Each of these elements can substantially impact the RCS and must be meticulously examined to accurately determine the actual RCS, which is conditional. (The configuration of the actual radar pulse is also important.)

The next plot shows the spectral response of a sphere with a diameter of four meters at Low Earth Orbit (LEO) altitude of 2000 Kilometers.

- The x-axis represents the wavelength of the radar waves, expressed in micrometers (micrometers). This axis spans a range of radar wavelengths used for detection, ranging from longer wavelengths (corresponding to lower frequencies) to shorter wavelengths (corresponding to higher frequencies).
- The y-axis represents the radar cross-section (RCS) of the sphere, which is a measure of how much electromagnetic energy is scattered back towards the radar receiver. The RCS is expressed in square meters (square meters).

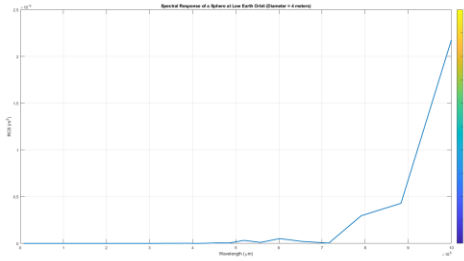


Figure 3 the Spectral Response of the sphere with 4Meters diameter - 300 MHz to 40 GHz

Analyzing this plot reveals the variation in the Radar Cross Section (RCS) of the sphere across different radar wavelengths. Peaks or dips in the plot indicate wavelengths where the sphere reflects radar waves particularly strongly or weakly. This insight is vital for comprehending the sphere's interaction with radar waves across the electromagnetic spectrum, aiding in the design and optimization of stealth technology to reduce radar detection. It is important to note that the sphere used in this example is a simplified model meant to illustrate the concept.

The next plot shows the spectral response of a sphere with a diameter of four meters at different altitudes (2000 kilometers, 5000 kilometers, and 10,000 kilometers) Representing Different Orbits.

- X-axis (Wavelength): Represents the radar wavelength, measured in micrometers (micrometers). It spans a range of wavelengths corresponding to radar frequencies from low to high.
- Y-axis (RCS): Represents the radar cross-section (RCS) of the sphere, measured in square meters (square meters). This indicates how much electromagnetic energy is scattered back towards the radar receiver.
- Lines: Each line on the plot corresponds to a different altitude. Specifically, the altitude of each orbit is labeled in the legend.

The plot shows how the RCS of the sphere varies with different radar wavelengths at various altitudes. Peaks or dips in the plot indicate wavelengths at which the sphere exhibits particularly strong or weak radar reflection.

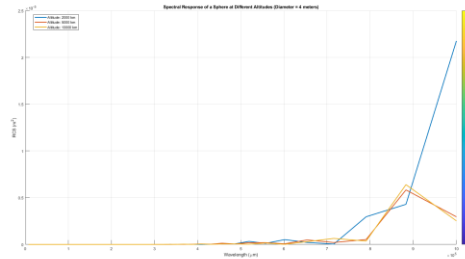


Figure 4 Spectral Response of a Sphere at Different Altitudes (Diameter = four meters)/300 MHz to 40 GHz

By analyzing this plot, one can gain insights into how altitude affects the spectral response of the sphere, and how specific radar wavelengths are absorbed, transmitted, or scattered by the sphere at different altitudes.

Next plot illustrates the spectral response of a sphere with a diameter of four meters at different altitudes (2000 kilometers, 5000 kilometers, and 10,000 kilometers), considering the respective orbital velocities of the orbits.

- X-axis (Wavelength): Represents the radar wavelength, measured in micrometers (micrometers). It covers a range of wavelengths corresponding to radar frequencies from low to high.
- Y-axis (RCS): Represents the radar cross-section (RCS) of the sphere, measured in square meters (square meters). This indicates the amount of electromagnetic energy scattered back towards the radar receiver.
- Lines: Each line on the plot corresponds to a different altitude, with the altitude labeled in the legend. Additionally, the orbital

speed of the sphere at each altitude is provided in the legend.

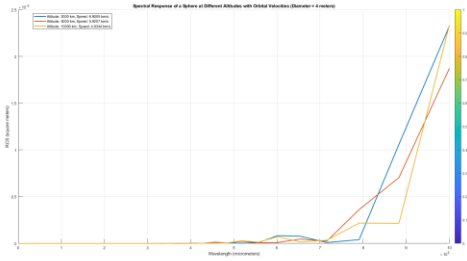


Figure 5 Spectral Response of a Sphere at Different Altitudes with Orbital Velocities (Diameter = four meters)

The plot demonstrates how the RCS of the sphere varies with different radar wavelengths at various altitudes, considering the Doppler shift effect induced by the orbital velocities. Peaks or dips in the plot indicate wavelengths at which the sphere exhibits particularly strong or weak radar reflection.

By analyzing this plot, insights can be gained into how altitude and orbital speed influence the spectral response of the sphere, and how specific radar wavelengths are absorbed, transmitted, or scattered under these as mentioned earlier, the configuration of the radar pulse is crucial. The simulations provided above are general and do not consider a specific radar pulse, as this would vary depending on the capabilities of potential adversaries.

Additionally, the materials used in satellite construction are important due to the harsh conditions of space. Satellites experience rapid temperature fluctuations, particularly when transitioning from the shadow to the sunlight side of Earth. While lightweight composite materials (LCMs) are recommended, it is essential to select materials with the correct composition for the satellite frame. For example, materials like GSD24, introduced in Nightshade, are designed to withstand these conditions.

Moreover, the chosen composite material should shield the satellite and its critical subsystems from background radiation resulting from space weather conditions and potential man-made electronic, microwave, laser, and electromagnetic bombardment attacks.

I personally would not recommend the use of Radar Absorbing Materials (RAMs) in satellite design unless the material is uniquely developed to be lightweight. The use of RAM in spaceborne assets is somewhat irrelevant yet not entirely impractical. This specific subject requires extensive research and development. One reason I do not advocate for the use of RAMs in satellites is the added weight of the material to the finished design. While RAMs are indispensable to the configurations of stealth jets and bombers, their use would be problematic in maintaining weight and cost, not to mention the cost of orbital deployment.

Next is incorporating active stealth components into the Satellite. The use of active stealth components is the most valuable tool in stealth design for satellites. Active stealth components are more practical due to the fact that they can cover a large portion of the spectrum (based on their design and capabilities). This would enable spaceborne assets to avoid detection from a wide range of adversarial surveillance systems. However, one must understand that since satellites are positioned in orbit, they are being surveilled by a large composition of radars from almost every nation on this planet. This wide range of surveillance force and focus should be taken into account, and correct configurations must be applied for accurate processing and countermeasures. There are fundamental differences when designing an active component for a satellite compared to a plane.

The detection method dictates the use of a wide array of terrestrial-based assets to

detect and proceed with the optical detection of spaceborne assets. The use of the concept of terrain masquerading is a viable countermeasure to combat optical detection of spaceborne assets. Digital camouflage will give the satellite the symmetry it requires to combat optical detection. The use of Light Absorbing Materials (LAMs) is encouraged to mask the satellite with the terrain in order to create advanced optical camouflage to combat optical detection and visual information gathering from the asset.

The signals that the satellite propagates and receives are used to identify the satellite communications. Telemetry and communication masquerading are not only contributing to hardening of spaceborne assets against adversarial attacks but will also contribute to force protection and redundancy. The use of techniques such as FHSS (Frequency Hopping Spread Spectrum) as well as randomizing communication channels and developing next-generation encryption protocols and signal masquerading will guarantee operational continuity and uphold the principles of force protection as well as hiding the satellite's communication signatures. Signal masquerading is crucial to ensure minimizing the electronic signature of satellites and other spaceborne assets. Remember that satellite communication is still a wireless broadcast and anyone with adequate hardware can listen or collect sample data for further processing.

As I stated earlier, "STEALTH" is a mantra of techniques and technologies that contribute to the subject in discussion. Due to the sensitivity of the subject, I withheld critical information and design components, but I expect readers to understand the subject in discussion and expand the idea in the interest of the United States. My point of view has always been to ensure and guarantee the absolute superiority of the United States, and this paper is dedicated to

the United States Space Force, aiming to take another step toward that objective.

Introducing Spaceborne Mission Control Hubs (SMCH)

As we delve into the subject of detecting spaceborne assets, a major aspect is identifying their communications and telemetry. Observing the orbital layers, Nightshade dictates the utilization of higher orbits to create space-borne mission control platforms for consolidation, masquerading, and backup. (We are not talking about orbital relays.)

This can be utilized to create a communication "HUB" or "Router" for stealth satellites, avoiding direct communications with ground stations. The SMCH (Spaceborne Mission Control Hubs) will act as routers to communicate with stealth spaceborne assets. Note that while introducing this methodology, it does not imply all assets will no longer have direct communication capabilities with ground stations and mission controls. Instead, it adds another layer of protection and redundancy. If targeted by jamming or cyber-attacks, the relay network can maintain access and communications with the assets and vice versa, creating an effective EMCON (Emissions Control) Strategy to uphold the stealth aspect of the communications.

We should never lose access or communications with spaceborne assets. The principle of force-protection dictates that redundancy is key to survival. As seen, there is much more to integrating and incorporating stealth into orbital assets than presented.

Developing a stealth asset requires protecting its secrets. Just because an asset has stealth capabilities does not mean we can abandon it. The concept has shifted to

developing the next generation of spaceborne military networks. I refrain from expanding this subject due to its sensitivity and because this is a public release.

This concept minimizes communications from stealth assets but never aims to create a centralizing platform which can be easily targeted. Each asset maintains redundant and independent channels for backup communications, aiming to minimize electronic signatures.

Avoiding a centralized infrastructure without redundant protocols is essential. In the event of a targeted attack against the centralized master asset, you lose access to slave assets. Therefore, each asset maintains its own redundant communication protocols with mission controls on Earth. Assets only communicate with the SMCHs, which acts as a centralized hub for communication with mission control. To mitigate risks, increasing the number of SMCHs in upper and lower orbits ensures multilayered redundancy, but ensuring all assets have redundant communication protocols is paramount. Additionally, this will introduce the concept of a shadow network for communications with the assets.

In the event of orbital suppression attacks, only fixed and mobile terrestrial redundancies ensure survivability and continuity of ISR, communications, and strategic capabilities. Besides, in the event of deploying a nuclear anti-satellite device, orbit disruption and catastrophic damage occur to strategic assets, along with debris dispersion into higher orbits. These primary effects, along with secondary effects like HEMP effects or ionization of the atmosphere, could result in a communications blackout. Therefore, regardless of incorporated technology or novel concepts, maintaining redundant terrestrial capabilities is the most important defensive strategy against adversarial interruptions.

Adapting the Use of Active Spaceborne Decoys

Perhaps one of the greatest concepts that Nightshade has introduced is the use of active decoys and countermeasures, from cyber operations to satellite and spaceborne warfare. We use decoys in our terrestrial military operations all the time, and most existing decoys are passive. Night Shade introduced the use of active terrestrial and spaceborne decoys. Unlike terrestrial decoys, spaceborne decoys are much more expensive to deploy also passive decoys are easy to detect if we take the full-detection cycle into consideration.

Active decoys can mimic the behavior of an asset via pre-recorded means. They could mimic the behavior and electronic emissions of satellites to divert the focus of adversaries toward the decoys rather than the stealth assets. Creating stealth assets does not mean you can leave them in the wild. Remember, Stealth is the mantra of techniques, some are asset-related, and other strategies relate to tactics. These assets, while emitting signals, are still managed by EMCON (Emissions Control) protocols and still have to communicate with a ground station and transmit scrambled data to register as active assets to adversaries.

The fact that they have to mimic a satellite's behavior means they have to have some form of electronics onboard, which means a costly asset. Note that decoys must be present in your networks. Passive decoys have little to no place in orbit, unless we consider making a hybrid decoy, which is less complicated and costs less. Active decoys, however, are a whole new concept and scenario. They can be used for deception campaigns and the protection of stealth assets in space. The use of such decoys would degrade adversarial detection capabilities and create a much-needed fog of war in space. As always, it is

only fair to assume that adversaries would use the same principles for deploying decoys, and therefore the advancement and perfection of the detection cycle are required to ensure full detection and classification of adversarial capabilities.

References:

- Enayati, Adib. (2024). The Mechanics of Spaceborne Warfare: Exploring Anti-Satellite Operations. 10.13140/RG.2.2.32664.00005.
- Enayati, Adib. (2024). Mechanics of Spaceborne Warfare: Redefining Orbital Suppression Dynamics. 10.13140/RG.2.2.26471.66725.
- Nightshade Advanced Polymorphic Defense and Warfare Doctrine, by Adib Enayati, Ph.D. (Not Available for Public).
- Nightshade Advanced Polymorphic Defense and Warfare Doctrine, by Adib Enayati, Ph.D. (Not Available for Public)—Section 5, Spaceborne warfare and the associated spaceborne weapon systems and the proposed designs.
- Nightshade Advanced Polymorphic Defense and Warfare Doctrine, by Adib Enayati, Ph.D. (Not Available for Public)—Subsection 1. Principles of the spaceborne warfare Arbiter Framework—Electronic deterrence and the adaptive strike chain, Adib Enayati, Ph.D. —J Def Stud Resour Manage 2023, 11:1—1 February 2023, DOI: 10.4172/2324-9315.1000162—Manuscript No. JDSRM-22-81303 ®.
- Enayati A. (2023) Arbiter Framework and the Adaptive Strike Chain. J Def Stud Resour Manage 11:1. / 01 February, 2023, DOI: 10.4172/2324-9315.1000162