MARCH 2020

Wargaming U.S. Space Operations

A STELLA POLARIS MODEL

An Article by

JOHN KURRE
RESEARCH@16POINTS.NET

Abstract

Much of our daily lives are dependent on space technology currently orbiting the Earth. Satellites operating television signals, emergency transmissions, weather reporting, global positioning systems, military surveillance, and other dual-use technologies are not only incredibly crucial to life on Earth but also to the defense of our nation. Space, once known to us as conduct for peaceful purposes, is now officially a war fighting domain. According to the United States Air Force, we intend to maintain space superiority, but to do that, we must have freedom from attacks and the freedom to maneuver. Due to these reasons, Space Situational Awareness (SSA) and Space Domain Awareness (SDA) is vital in protecting the United States space-based assets and all its interests in Space. In recent years, the United States uniformed services have simulated real-world scenarios depicting acts of war as part of their war gaming exercises. These exercises lead to improved military planning and decision-making capabilities for Military Space Operations that are crucial in maintaining the elasticity and security posture of the United States Space infrastructure.

Introduction

In recent years, the United States has become a victim of terrorism, cyber assaults, and a multitude of aggressors who continue to undermine and reject its democracy and geopolitical status. While the United States continues to battle these adversaries and enforce its comprehensive national security policies in the post-9/11 world, there has been an exponential increase of adversaries such as hostile nation-states and malicious threat actors who have targeted its economy, critical infrastructure, and overall digital footprint with Ransomware attacks, and Advanced Persistent Threats (APT). In the past two years, the United States has also suffered an assault over its election processes, rendering itself virtually vulnerable to sophisticated attacks in all spheres. Space is no different as it is also susceptible to a myriad of attack vectors, and degradation of space-based capabilities like communications, navigation, and surveillance can be catastrophic to national space services as well as its defense.

There are 14 Spacefaring nations that are capable of building and launching vehicles beyond the Earth's atmosphere. They are U.S., U.K., Russia, China, Iran, North Korea, France, Canada, India, Japan, Israel, New Zealand, Ukraine, and South Korea. A multitude of attack options such as Satellite Jamming, Laser Weapons, Anti-Satellite Missiles, On-Orbit testing, Cyber Intrusions, and Physical Attacks to Ground-based space infrastructure (e.g., radars, telescopes, signals intercept antennas, and sensors) could disrupt, damage, destroy or deny crucial space-based civil and military services rendering space-based assets unusable.

Another big concern is the threat from orbital debris due to the congestion in Space and incidents either warranted (self-destruction or decommissioning) or unwarranted (launch failures, accidents or a deliberate attack on space assets) can lead to orbital debris creating a chain reaction and degrade space capabilities for all of the nations mentioned above.

This space security model pays homage to the existing process quality, predictive analysis, and process quality models used by many of the large-scale enterprises to identify and improve defects in the overall process, security posture as well as forecast future outcomes before an asset failure or an adversary attack. We will use a modified Six-Sigma process quality model called the *Stella Polaris Model* as a basis for improving the Space Security Posture using real-world data as well as samplings from a simulation.

To make this report easily understandable, we will use data from U.S. space history and variables that represent potential threat factors that can impact U.S. space-based assets leading to degradation of services and indicators that require improvement (defects). Space-based incidents for other countries are out of scope for this report.

An Overview of the Stella Polaris Model

The *Stella Polaris Model* conceptualized on March 3, 2020, in the hindsight of the rapid advancements made in the space industry. There are numerous theories and models developed by the scientific community on war and peace, but the idea of a predictive model such as Stella Polaris based solely on space security may intrigue strategic leaderships around the world to develop situational awareness in the space domain.

The model can be used both for qualitative and quantitative research purposes, especially in understanding the multinational footprint in the realm of Space and identify defects (Key Performance Indicators Critical to Quality). For a strategic security specialist, this model will help in analyzing historical challenges in launches, threat intelligence, enhance Space situational awareness, and rule out any potential threats from antagonists like Russia, China, Iran, and North Korea.

Disclaimer: The content in this document is not endorsed or approved by the United States government or any aerospace business or entity but is purely for academic research writing.

Methodology

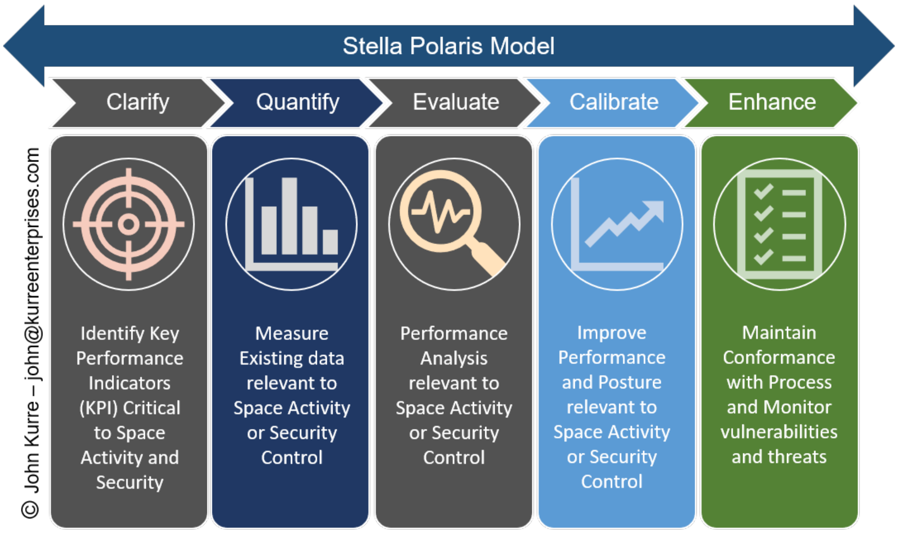


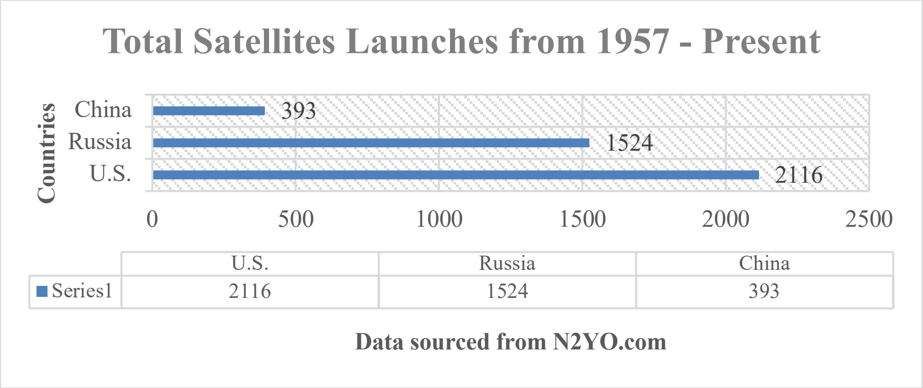
Figure 1: Stella Polaris Model

As you can see from the above image, the Stella Polaris Model is a five-phased process. We will first use the model against United States Astronaut Spaceflight and Astronaut Training Programs conducted in years between 1960 – 2019. We will observe the areas of opportunity (defects) and provide recommendations for improvements in these programs.

Then we will move onto simulated exercises using real-world Counterspace Threats against the United States Space Infrastructure to search for the areas of opportunity and to provide recommendations based on our observations.

Phase 1: Clarify

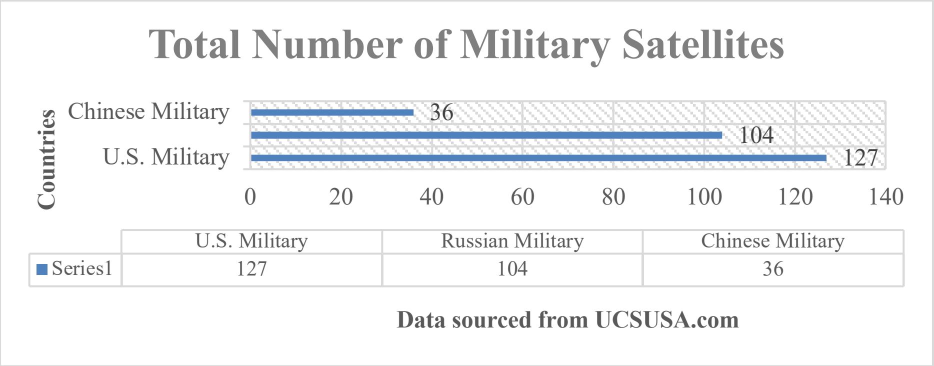
Key Performance Indicators (KPIs) that are critical to space activity or services are known as defects. We must first take a look at Space-based services deployed in orbit. In this case, we will take a look at the total number of assets deployed in Space by the United States, Russia, and China. These can include communications, navigation, weather, reconnaissance, and remote sensing satellites.



	U.S.	Russia	China
■ Series1	2116	1524	393

Data sourced from N2YO.com

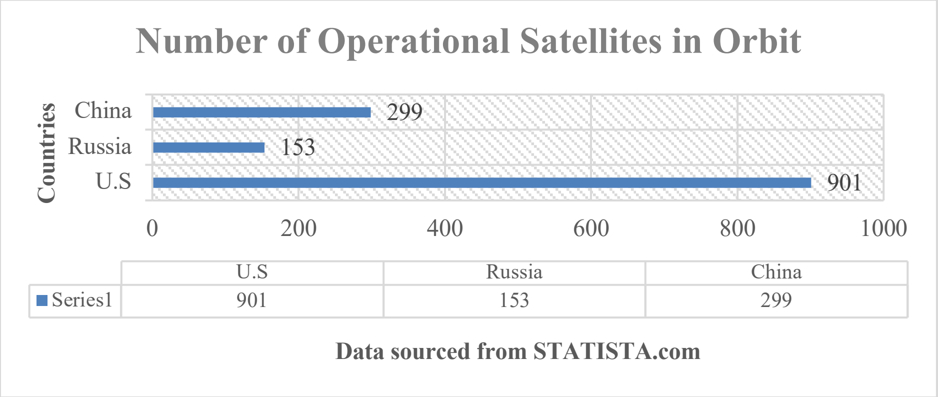
Figure 2: Total Satellite Launches - U.S. Russia and China



	U.S. Military	Russian Military	Chinese Military
■ Series1	127	104	36

Data sourced from UCSUSA.com

Figure 3: Total Military Satellite Launches - U.S. Russia and China



	U.S	Russia	China
■ Series1	901	153	299

Data sourced from STATISTA.com

Figure 4: Total Operational in orbit - U.S. Russia and China

According to the *Figures 2, 3, 4*, the United States has launched 2116 satellites since 1957 and out of the 2116 satellites, 127 satellites are solely for Military use. Although the United States has launched a large number of satellites, the number of satellites in orbit is lesser than the total number of satellites launched, and this can be attributed to disasters such as launch-related failures and rocket explosions. The same variable applies to the other two countries, but for the remainder of the model stages, we will focus only on U.S. based space services and assets deployed.

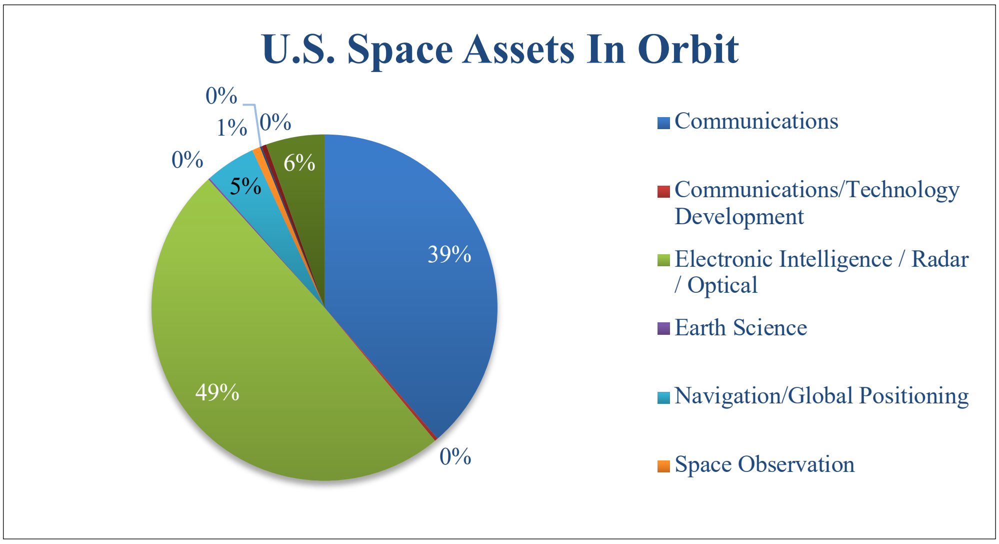


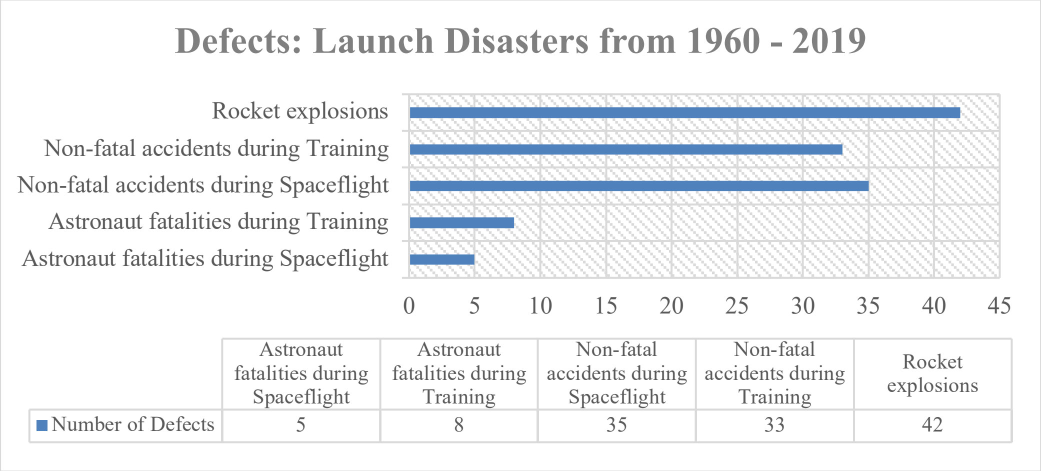
Figure 5: U.S. Space Assets in Orbit

Phase 2: Quantify

In the second phase of this model, we will quantify available data related to disasters, threats, space weapons in orbit, and a multitude of counterspace threats that could suddenly shift from peaceful use of Space to a full-scale attack potential. We will require space activities data to understand the overall risk posture of United States readiness, security, and activities in Space.

It is crucial to remember that the inability to launch a spacecraft or satellite into orbit is called a Defect, and these are attributed to launch disasters, accidents, malfunctioning equipment, or satellite failures. Any attempt or action with the capability, means or intent to disrupt, deny and destroy space base services is called a Counterspace Threat. Any military technology capable of attacking targets in Space from Earth or attacking targets on Earth from Space is called a Space Weapon.

Aerospace Disasters: *Figure 6* displays the number of launch-related defects attributed to Astronaut Fatalities. There were 5 Astronaut fatalities reported during Spaceflight, 8 reported during Training, 35 Non-fatal incidents reported during Spaceflight, 33 Non-fatal incidents during Training, and a total of 42 Rocket explosions during launch.



	Astronaut fatalities during Spaceflight	Astronaut fatalities during Training	Non-fatal accidents during Spaceflight	Non-fatal accidents during Training	Rocket explosions
■ Number of Defects	5	8	35	33	42

Figure 6: Launch Disasters Recorded from Astronaut Spaceflights and Training

Counterspace Threats: The altitude at which each spacecraft orbits vary from each other depending on their civil-military specifications and operational use. There is sure existence of a plenitude of threats to satellites in orbit, and these can be attributed to the use of space weapons, jamming satellite frequencies, cyber-attacks, direct energy weapons, ground-based attacks, electronic warfare, human-made threats, kinetic energy weapons, X-ray laser beams and numerous other orbital threats. Any potential to disrupt, deny, degrade or destroy space services is called an orbital threat. Orbital debris is also a major concern and falls under the category of orbital threats.

Space Weapons: The United States is heavily dependent on its space services for communication, navigation, weather, and other civil-military workloads, and any deliberate attempt to degrade or disrupt these services can have a profound impact on its civil-military interdependencies. As spacefaring nations become capable of launching undisclosed payloads into orbit, Space continues to become more congested with numerous opportunities as well as threats. Space Weapons are developed to protect and defend critical infrastructure in space stationed either on the ground or in orbit.

These Space weapons are commonly known as ASATs or air-launched anti-satellite multistage missiles or anti-satellite weapons in general. ASAT falls under the category of

Kinetic Energy Weapons (KEW). KEWs are capable of being launched from a ground base or orbit, and their purpose is to target rogue fragments, objects, or hostile satellites with a trajectory to pinpoint and destroy its targets. *Figure 7* displays a list of real-world Space Weapons at the disposal of the United States.

Figure 7: U.S. Space Weapons

Phase 3: Evaluate

In this stage of the process model, we will analyze and validate the data collected in the previous phase, find the root cause for astronaut fatalities and also simulate an attack on space-based assets to arrive at a hypothesis.

Aerospace Disaster Analysis:

The scope of this analysis is to validate astronaut fatalities reported from Spaceflight and Training programs between the years 1960 – 2019. Here, our goal is to determine the maximum number of fatalities in each program. Since our goal is also to determine the root cause of each fatality and reduce such fatalities in future Astronaut Spaceflight and Training Programs, we will consider them as reduction of defects to the process.

Astronaut fatalities during Spaceflight is a Key Performance Indicator (KPI) in the Astronaut Spaceflight Program, and all fatalities are specific only to one occurrence and are isolated in nature. Meaning, they have occurred only once during the Astronaut Spaceflight Program life cycle between the years 1960 -2019. In this scenario, we don't have much data to work with, so we must continue analyzing other parameters.

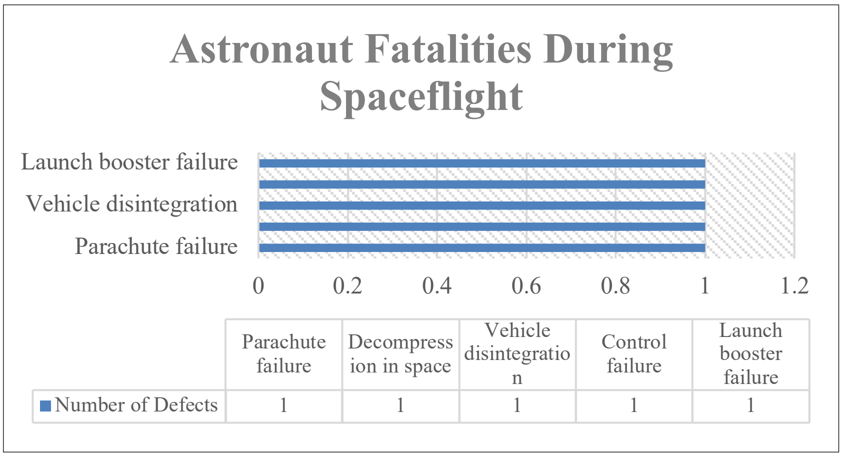


Figure 8: Astronaut Fatalities Recorded during Spaceflight

Astronaut fatalities during Training is a Key Performance Indicator (KPI) in our Astronaut Training Program, and there are 4 Jet Crashes reported, 1 unfortunate incident related to Drowning, and 3 incidents related to Fire and Explosion. *Figure 9* shows that during the life cycle of the Astronaut Training Programs between the years 1960 - 2019, Jet crashes and Fire explosions had the maximum number of defects.

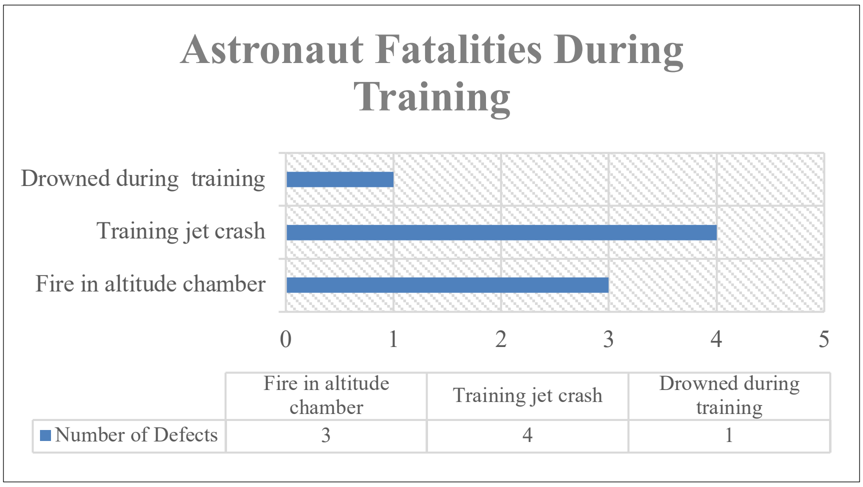


Figure 9: Astronaut Fatalities Recorded during Training

Non-fatal accidents during Spaceflight is a Key Performance Indicator (KPI) in the Astronaut Spaceflight Program, and it has a total of 35 non-fatal accidents (defects). Upon analyzing the data between the years 1960 -2019, the non-fatal accidents were reported due to 9 incidents from Equipment failures, 4 incidents from Separation failures, 3 casualties were reported from Drowning and 3 accidents from Spacesuit or airlock design failure. The remainder of the defects occurred only once during the program life cycle and are considered non-reoccurring isolated events.

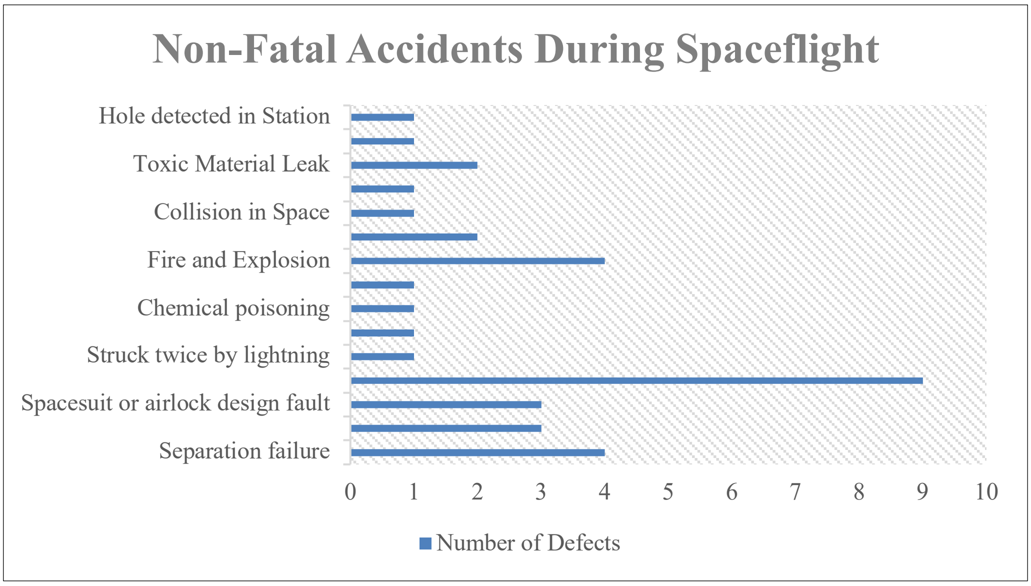
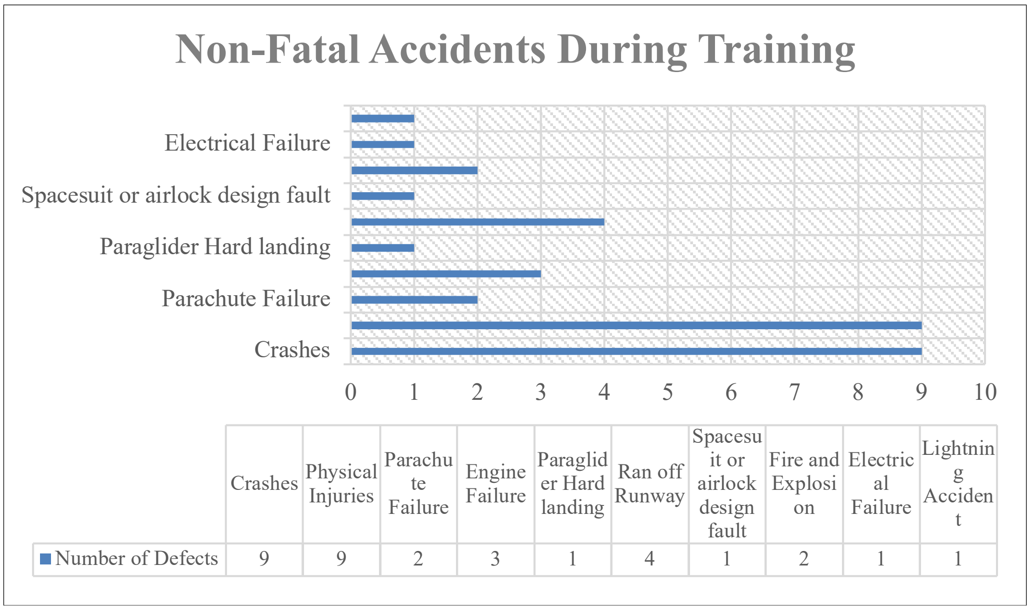


Figure 10: Non-Fatal Accidents Recorded during Spaceflight

Non-fatal accidents during Training is a Key Performance Indicator (KPI) in our Astronaut Training Program, and it has a total of 33 defects. Upon analyzing the data, it was observed that between the years 1960 -2019, Training related Physical Injuries occurred from 9 separate incidents, followed by 9 more distinctive incidents related to Training related Jet Crashes. Jets that ran off the Runway reported 4 accidents, Electrical Failure reported 3 accidents, and there were 2 Fire-related casualties. The remainder of the defects, including lighting strikes, thankfully occurred only once and were non-reoccurring isolated events.



	Crashes	Physical Injuries	Parachute Failure	Engine Failure	Paraglider Hard landing	Ran off Runway	Spacesuit or airlock design fault	Fire and Explosion	Electrical Failure	Lightning Accident
■ Number of Defects	9	9	2	3	1	4	1	2	1	1

Figure 11: Non-Fatal Accidents recorded during Training

There were 42 incidents reported from Rocket Explosions due to production faults, making it the most severe concern for quality improvement.

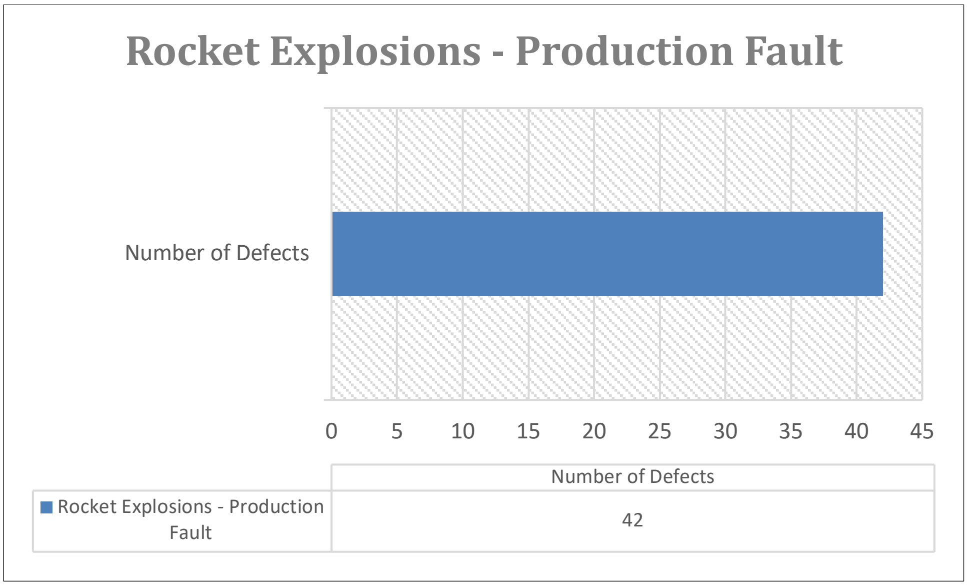


Figure 12: Rocket Explosions recorded between 1967 – 2019

Now that we have validated Astronaut Spaceflight and Training related Disaster-data, it is time we investigated Counterspace Threats and how they measure in terms of our overall space readiness and existing national space security posture. Some of the sample data is to challenge our space battlefield readiness, but in a real-world scenario, an attack on a Space-based asset would be catastrophic.

Space Weapons and Counterspace Threats. The Space Weapons graph shows that the United States Navy maintains most of the arsenal totaling at 100+ Sea-based M3 missiles to protect assets in orbit. There are 2 interceptors maintained by the U.S. Army and Missile Defense Agency. There are 6 Advanced Technology Risk Reduction Satellites and 2 Micro Satellite Technology assets deployed in Space and in orbit.

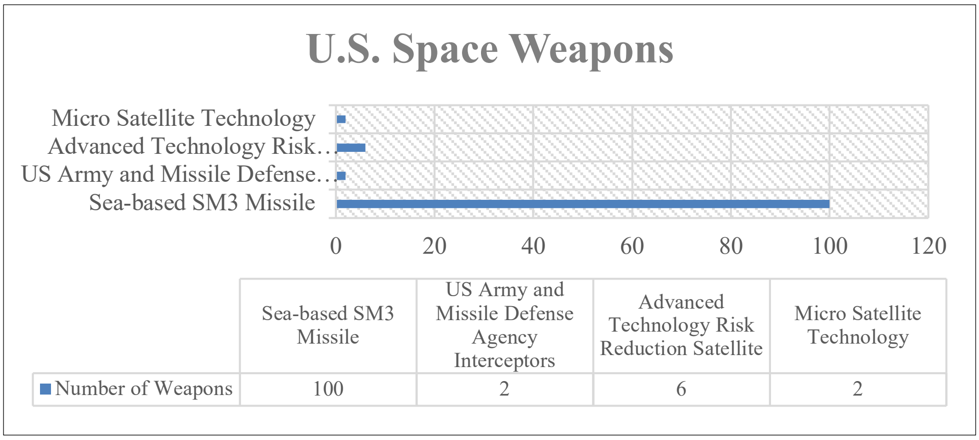


Figure 13: U.S. Space Weapons

The Counterspace Threats graphs are a simulation of incidents associated with threats against U.S. Satellites. The Damage Potential signifies how critical these counterspace threats are, and irrespective of the number of Anti-Satellite weapons deployable from Earth or Space, any attack on a satellite becomes irreversible rendering space services permanently unusable. For example, a Nuclear Detonation in Space would have catastrophic consequences if deployed, but the time it takes to intercept such a threat is dependent on Space Situational Awareness and the ability to identify, detect, distinguish and destroy counterspace threats is of utmost importance not only to establishing battlefield readiness but also in gaining space superiority.

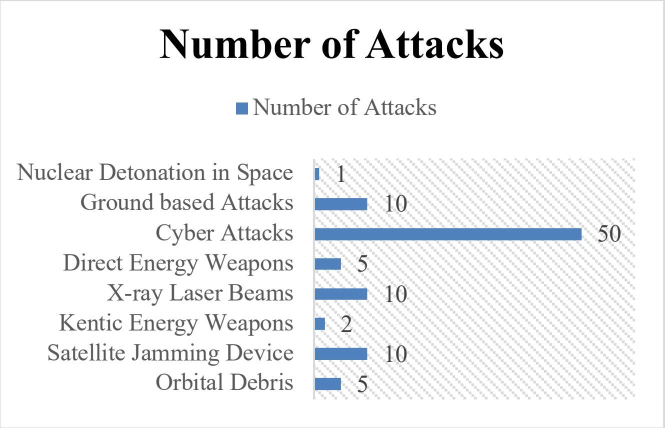


Figure 14: Number of Orbital Attacks

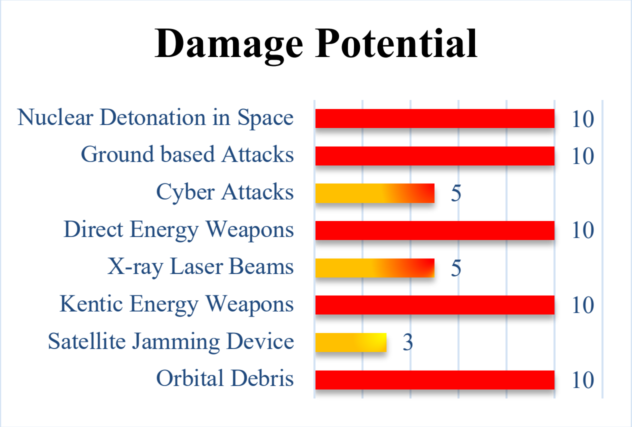
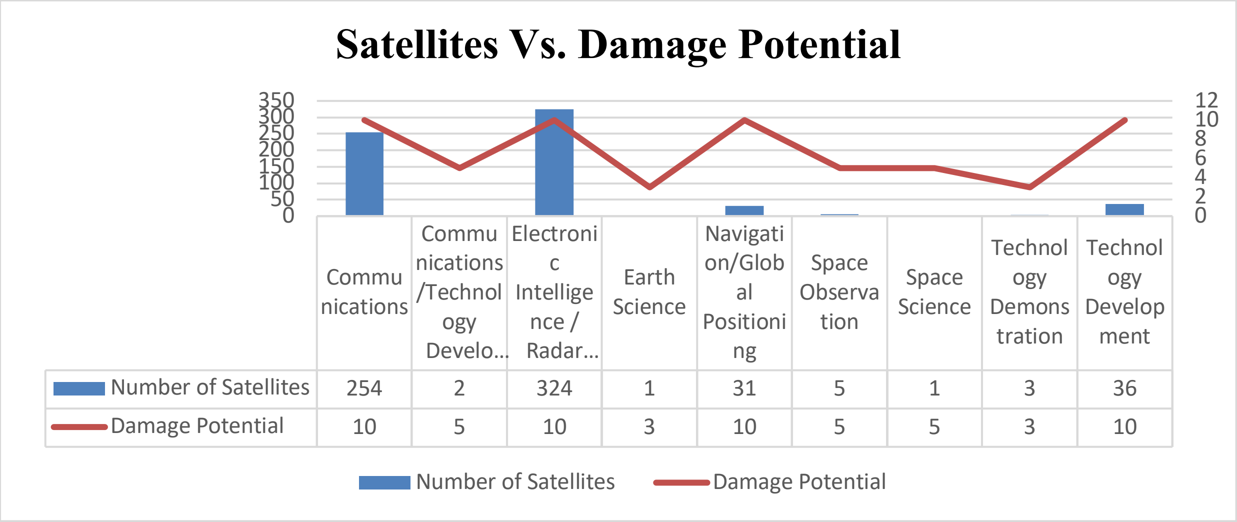


Figure 15: Damage Potential of each Orbital Attack



	Communications	Communications/Technology Develo…	Electronic Intelligence / Radar…	Earth Science	Navigation/Global Positioning	Space Observation	Space Science	Technology Demonstration	Technology Development
Number of Satellites	254	2	324	1	31	5	1	3	36
Damage Potential	10	5	10	3	10	5	5	3	10

Figure 16: Satellites Vs. Damage Potential of Orbital Attacks

Phase 4: Calibrate

In this stage of the process, we will determine the root causes of the defects that have occurred during Astronaut Spaceflight and Training Programs between the years 1960 – 2019. The calibrated data will provide us with proper recommendations to implement process or program quality controls to mitigate future occurrences.

Astronaut Fatalities During Spaceflight: As shown in *Figure 8* there were only 5 isolated incidents that occurred once during its lifetime. Issues related to Launch boot failure, Control Failure, Vehicle Disintegration, Decompression in Space, and Parachute Failure, happened only once, causing fatalities to Astronauts. In this scenario, we don't have much data to work with, so we must continue analyzing other parameters.

Astronaut Fatalities During Training: As shown in *Figure 9* there were 3 significant defects identified that caused the fatalities during the Astronaut Training Program. In the order of priority, Training Jet Crashes reported 4 deaths, Fire and Explosion reported 3 fatalities, and 1 death caused by Drowning.

Non-Fatal Accidents during Spaceflight: As shown in *Figure 10* there were 35 incidents that were related to non-fatal accidents during the Astronaut Spaceflight Program. Multiple occurrences of an incident are a cause for concern as minor accidents could lead to fatal accidents, and process improvement procedures must primarily focus on reducing accidents. In the order of importance, there were 9 separate accidents caused due to Equipment failure, 4 due to Separation failure, 4 due to Fire and Explosion, 3 accidents reported due to Drowning, 3 due to Spacesuit or Airlock Design Fault, 2 Physical Injuries and 2 due to Toxic Material leak. Other incidents took place only once and were isolated events.

Non-Fatal Accidents During Training: As shown in *Figure 11* there were a total of 33 accidents that took place during Astronaut Training Program. In the order of importance, 9 occurred due to Jet crashes, 9 were Astronaut related Personal Injuries, 4 accidents due to vehicles Running off the Runway, 2 related to Fire and Explosion, 2 related with Parachute Failure, and 3 with Engine Failure. Others were isolated events and can go through further calibration to check for dependency on other activities.

Rocket Explosions: As shown in *Figure 12* there were 42 explosions related with production fault, and all of the explosions caused severe injuries and fatalities. In the next stage, we will identify activities that require enforcement of higher quality control to avoid the risk of explosions and loss of life. Any event, either an incident, accident, warranted, or unwarranted that causes loss of life, is high risk and must be scrutinized with a top priority.

Counterspace Threats and Attack Simulation: In this section, we will perform a simulated attack on U.S. Space-based assets in orbit to determine readiness and space situational awareness. Before we get into the next stage of the process, we will take a look at a space-based conflict from a war gaming perspective. Here, we will identify the Types of Satellites, Damage Levels, Simulate Counterspace Threat Attacks, and finally calibrate the actual damage to Space Infrastructure. In the next and final stage of the process, we will discuss areas of opportunities and enhancement of Space Operations for the continued security of our Space-based assets.

Figure 5 is a real-world representation of U.S. space infrastructure. The data was extracted from the USC Satellite Database and features real time information of 2218 satellites owned by the United States and 657 satellites in orbit. The graphs are limited only to U.S. based satellites that are in orbit.

There are myriad of data sources, and each tells you a different story on the actual number of satellites in Space. For this report, the USC Satellite Database is the primary data source for all Satellite information. *Challenges to Security in Space*, by the Defense Intelligence Agency, was an excellent resource for Counterspace Concepts and Threats.

Space is now a warfighting domain and consists of a multitude of threats and attack vectors listed below:

Orbital threats: Any system deployed for non-peaceful purposes in an attempt to destroy a space-based asset is called an orbital threat. Orbital threats include man-made threats, attacks from space weapons, or even space debris that can cause damage and destruction to spacecraft and satellites.

Cyber Attack: Any system or a distributed network of systems used by an actor to disrupt, deny, deceive or degrade space services, such as a denial of service (DoS) attacks to overload the system, and to render it incapable, by hacking or spoofing is called a cyber-attack.

Satellite Jamming: Preventing users from receiving signals by jamming a satellite's frequency.

Space Weapons: Weapons designed to produce reversible or non-reversible effects against space systems such as destroying or damaging space sensors, robotic systems, lasers, kinetic energy weapons, direct energy weapons, and all militarized threats.

Nuclear Detonation in Space: The launching of an Intercontinental Ballistic Missile with Nuclear Warhead capability into Space to attack space-based systems.

Ground-based Attack: Attacking ground-based communications and satellite operations by physical means.

The *Figures 14, 15 and 16* display a wargaming simulation of an attack on U.S. Space Infrastructure. The following Counterspace Threats have Space Conflict Levels or Damage Level Potential. We have also simulated a specific number of attacks using a counterspace threat to each category of satellites. A Damage Potential assigned depicts a hypothesis of the aftermath.

The Satellite Vs. Damage graph clearly shows some categories of satellites consists of a greater pool of satellites in orbit, whereas others consist of fewer numbers. For example, there are 254 Communication satellites, and they have a high Damage Potential not only because of internetworking of the larger pool but also because of the civil-military dependency on these satellites. It is crucial to note the Damage Potential of 10 is catastrophic since it disables the operational capabilities of all Communication satellites. That said, any destruction caused to satellites creates orbital debris, turning them into space junk travelling at a velocity of 18,000 miles an hour towards other satellites currently in orbit.

This is just one example, but it otherwise showcases how vulnerable Space is, and any attempt to destroy or attack a space object like a satellite can be disastrous for not just one country but also for other Spacefaring countries.

In the next stage of the process, we will provide recommendations for a security specialist to improve Space Situational Awareness and Space Domain Awareness for the proper defense of Space Objects. Please understand this is a condensed version for academic purposes. Still, a variety of simulations can be performed using this model to arrive at a much broader consensus depending on the test scenarios and strategize space security doctrines as per the user's discretion.

Phase 5: Enhance

Spaceflight Disasters:

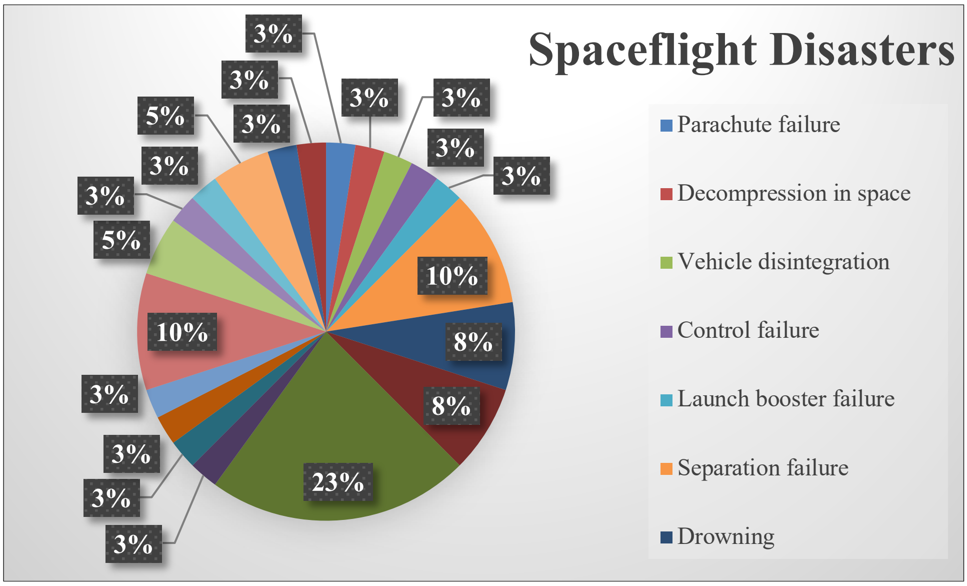


Figure 17: Spaceflight Disasters

Figure 17 above displays that 23% of significant defects or disasters in this program are related to Equipment failure. The Astronaut Spaceflight Program must take adequate measures in establishing a robust procurement process that is quality intensive and integrated with other capability maturity models. As technology advances, much of the value of such equipment also depreciates. Budgeting for a higher Return on Investment (ROI) before grading its current quality of service and standards impacts decision planning for future year road map. Business processes must be adopted as per regulatory requirements and standards, and adherence to such requirements and standards must also apply to vendors and equipment manufacturers throughout the program pre-solicitation and post-solicitation process.

Over many years the Aerospace industry has made significant improvements and developed its organizational processes based on technological advances. However, the data is based on programs that were established in the early 1960s and may require a high degree of scrutiny due to quality defects or disasters associated with equipment failures.

Training Program:

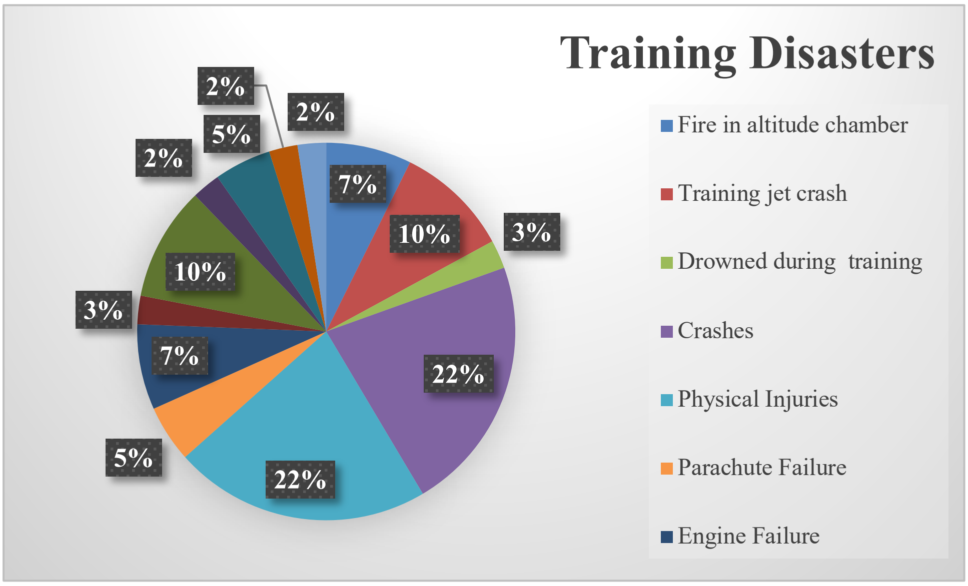


Figure 18: Training Disasters

Figure 18 displays 22% fatalities reported from Physical Injuries in the Astronaut Training Program, and 22% of deaths related to Jet Crashes. Here, it does seem like there is a data spike correlated with human error. Equipment malfunction or failure could have also caused Personal Injuries or Operator Error. The same applies to Jet Crashes; most of the crashes are a combination of operator errors and equipment malfunction. That said, several instances indicate that fuel line ignition and engine failures were the ultimate cause for Jet crashes, leading up to the unfortunate fatalities. Organizations must develop an efficient life cycle process to accommodate product testing and achieve final certification on par with industry quality standards. Another important consideration is that the agency must have a vested interest in its Risk Management and Capability Maturity Programs to evaluate its current posture continuously.

Looking at NASA's knowledgebase website, much effort has been put in recent years to improve training programs for astronauts. The advent of new technology has streamlined learning and development processes. Much focus has been given to testing related activities, and an enormous amount of testing of operator capabilities with technological capabilities continues to be a foundational effort for space agencies like NASA.

Counterspace Threats and Wargaming:

Since the data collected is mostly simulation of a wargame, the remainder of the document will provide recommendations for a space security specialist or enthusiast interested in enhancing space security posture.

It is quite evident that Space has become an integral part of many civilian and military activities. From the first step on the Moon to the thought of colonizing Mars, human beings have made tremendous advancements in the field of Astronomy and Space Science. These advancements made for the peaceful use of Space has become congested because of other spacefaring nations launching satellites for their own nation's civil defense purposes. Although it is incredible to learn how far we human beings have come along, these advancements also pose a variety of threats because not all actors want to consider Space for peaceful use and because of such reasons, the United States must always remain cautious and battle-ready to protect its interests and assets in Space.

According to Paul Szymanski of the Space Strategies Center, foundational space doctrine, automated battlefield management, and tactical decision-making capabilities must be developed to enable war fighters to fight and win the next space war.

Space Situational Awareness (SSA) is also vital because not only will it help in monitoring and satellite tracking, but it will help develop space sensor tasking and optimization by ranking space objects (operable and inoperable). We must share best practices from countries such as Russia and China that currently have extensive networks of ground-based sensors to monitor these activities along with providing them with intelligence on ballistic missile early warning system. SSA can be instrumental in averting denial and deception attacks where adversaries conceal their ground-based sensitive military operations when remote sensing satellites and reconnaissance satellites make an overhead pass over their airspace.

Conducting Space Wargames enables accurate testing of space strategies and tactics. For example, in the data above, we have seen how severity levels matter in the affairs of civilian and military space activities. Still, much of these wargames must be conducted as close to battlefield scenarios rather than just keeping it theoretical and a hypothesis. We must continuously test current posture against questions like, will there be an attack on space systems in the near future? How do international relations influence our security in Space as well as at home front? Are the Space Systems already under attack? What type of deterrence do we have in place? Will GPS and other communication dependent services function during the war?

Space Operations must continue gathering intelligence to perform threat warnings and assessments. The rules of engagement must be developed in adherence to proper space planning, accommodate space base research, and the law of armed conflict.

Recently there has been a surge of companies specializing in space traffic control. This will help in resolving the issues that we face concerning space congestion and orbital debris.

The recommendations listed above are brief, but there is much work that needs to be done in this domain, and we must continue observing the current trends, practices and patterns of other spacefaring countries. There have been no real-world incidents to gather similar data and create a baseline using this model, but without the proper Space Situational Awareness and Space Domain Awareness, it will become a challenging affair in the event of a real attack. Our United States Military and the National Security Council have developed national space strategies that provide us with a wealth of information on strategic battle plans in the event of an attack. I believe it all starts with analytical planning, and a wargame modeling tool like *Stella Polaris* may help in attaining a high level of readiness.

References

Challenges To Security In Space. (2019, October 1). Retrieved from https://bookstore.gpo.gov/products/challenges-security-space

Competing in Space (n.d.). U.S. Department of Defense. https://media.defense.gov/2019/Jan/16/2002080386/-1/-1/1/190115-F-NV711-0002.PDF

List of spaceflight-related accidents and incidents. (2020, January 28). Retrieved from https://en.wikipedia.org/wiki/List_of_spaceflight-related_accidents_and_incidents#Non-fatal_incidents_during_training

UCS Satellite Database. (n.d.). Union of Concerned Scientists. Retrieved from https://www.ucsusa.org/resources/satellite-database#.XG6yv3RKiUk