

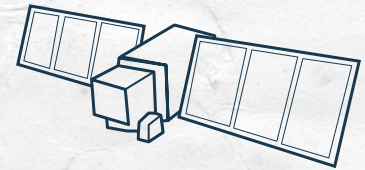

FEBRUARY 2021

A Report of the CSIS Aerospace Security Project

FOREWORD | Doug Loverro

AUTHORS | Todd Harrison, Kaitlyn Johnson, Makena Young

DEFENSE AGAINST THE DARK ARTS IN SPACE



Protecting Space Systems from Counterspace Weapons

FEBRUARY 2021

DEFENSE AGAINST THE DARK ARTS IN SPACE

Protecting Space Systems from Counterspace Weapons

FOREWORD | Doug Loverro

AUTHORS | Todd Harrison, Kaitlyn Johnson, Makena Young

A Report of the CSIS Aerospace Security Project

CSIS | CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES

**ROWMAN &
LITTLEFIELD**

Lanham • Boulder • New York • London

ABOUT CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

© 2021 by the Center for Strategic and International Studies. All rights reserved.

ISBN: 978-1-5381-4031-4 (pb); 978-1-5381-4032-1 (ebook)

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Rowman & Littlefield
4501 Forbes Boulevard
Lanham, MD 20706
301-459-3366 | www.rowman.com

ACKNOWLEDGMENTS

The team would like to extend our thanks to several key individuals who made this report possible. First, to Doug Loverro for his expertise, support with building the workshop scenarios, and writing of the foreword for this report. Second, to Emily Tiemeyer for her outstanding work on our Harry Potter-inspired layout, graphics, and charts. Third, to Jeeah Lee and Phillip Meylan for their expert eyes and copyedits. We would also like to thank our friend and colleague, Thomas Roberts, for his insight, contributions, and edits. Finally, the team would like to thank the space and national security experts who participated in the workshops that informed this study, which are discussed in Chapter 5 of this report.

This study was made possible by the generous support of the Smith Richardson Foundation and general support to CSIS.

The Aerospace Security Project would also like to recognize J.K. Rowling's *Harry Potter* series, which has greatly inspired our overall design concept, including the incorporation of its iconography and quotes.

While this report borrows the story and imagery of Harry Potter, we do not share the author's discriminatory views. The Aerospace Security Project team and CSIS support equality and representation for all, including the trans community, and we strive to create an environment where people of all backgrounds are heard and included. With the Harry Potter theme, we want to reaffirm some of the values the characters and stories taught us: friendship, courage, selflessness, and being true to oneself.

TABLE OF CONTENTS

Foreword.....	vi
CHAPTER 1: Space Is No Sanctuary.....	1
The State of Space Today.....	2
Militarization versus Weaponization of Space	2
Space Organizations	4
The Need for Space Defenses.....	5
Report Organization and Methodology.....	5
CHAPTER 2: The Dark Arts in Space.....	7
Kinetic Physical	7
Non-Kinetic Physical	8
Electronic.....	8
Cyber.....	9
CHAPTER 3: Space Defenses Defined.....	10
Defensive Counterspace Operations	10
Passive Defenses	11
Architectural Defenses	11
Technical Defenses	13
Operational Defenses.....	16
Active Defenses	18
Space-Based Defenses.....	18
Terrestrial-Based Defenses.....	20
CHAPTER 4: Space Defenses Applied	22
Objectives of the Attacker in Space	22
Objectives of the Defender in Space.....	24
Matching Defenses to Threats	25
CHAPTER 5: Scenarios for Defensive Counterspace Operations	27
Scenario 1: Russian Incursion into the Baltics	27
Scenario 2: Possible Hijacked Satellite.....	30
Scenario 3: Escalating Tensions in the South China Sea	31
Scenario 4: Commercial Space System Protection.....	34
Key Takeaways.....	35
CHAPTER 6: Conclusions and Recommendations.....	37
About the Authors.....	40

"All armies prefer high ground to low, and sunny places to dark . . . With regard to precipitous heights, if you are beforehand with your adversary, you should occupy the raised and sunny spots, and there wait for him to come up."

SUN TZU, THE ART OF WAR

FOREWORD

It is hard to imagine that Sun Tzu ever conceived of as "precipitous" a "height" or as "sunny" a "spot" as Earth orbit. But it is fascinating to wonder, if he had, would it have changed his perception of how battles would be fought and how wars could be won. Military theorists (and science fiction screenwriters) have often resorted to pronouncements taken from Sun Tzu to explain the basis of their decisions or to justify the boldness of their approach. But perhaps the true import of Sun Tzu's words is to operational commanders on how to best disposition forces and, more critically, how to identify the route to victory. If that is true, then clearly Russian and Chinese space strategists learned from a different Sun Tzu admonishment: "So in war, the way is to avoid what is strong and to strike at what is weak."

Since the turn of the century, the double-edged sword that space represents for U.S. forces has been apparent—it is

both a crucial advantage of U.S. military strength and a critical chink in the United States' military armor. The re-emergence of antisatellite activities around the world, and more specifically in Russia and China, was not due to sudden technological change but rather to the rising recognition of the changing strategic calculus of "what is strong" and "what is weak." More worrisome, the "weakness" of U.S. space forces is not limited to what happens in the heavens—losses there create new vulnerabilities on the ground, which then develop new nexuses of "what is weak" to attack.

The ideas in *The Art of War* are thought to be the compilation of generations of military learning from the experience of battle and that Sun Tzu, who may or may not have actually existed, compiled them into his eponymous text. He had the advantage of those generations of land conflict and the lessons from wars won and lost. Clausewitz and Mahan were similarly able to draw upon centuries of battle-tested plans and experiences to derive their own theories of land and sea strategy and to use those lessons to advance the state-of-the-art of doctrine, weapons, and employment of armed force. Unfortunately, we have no experience in space warfare to rely upon—no grand lessons of how force was applied nor even useful exercises to extend into actual combat. The slate is blank.

Certainly, the philosophical elements of war captured by Sun Tzu, Clausewitz, Mahan, and many others translate from domain to domain, but often that translation is fuzzy and subject to strategic surprise, especially when technology outpaces the application of derived concepts. The creation of the Maginot Line can be traced back to the writings of Sun Tzu on the superiority of the defense but was made technologically irrelevant by the introduction of air war-

fare. The "art of war" did not change, but its application needed to be amended. So too for space—the philosophical underpinnings are the same as they were 2,500 years ago—but applying those concepts to space conflict requires the ability to see beyond the grand concepts and into operational strategies and capabilities. That work has begun, but much more is required.

Into that fray comes this volume from the folks at CSIS. Outlining the development and possible types of the weapons of space conflict and some of the early existing strategic ideas that have been posited for how space conflict will evolve, they then put those ideas to the test. Through a series of thought exercises, marked by far more realistic scenarios than are often used in such endeavors, they seek to enlighten that which can only truly be learned in conflict. The results are simultaneously informative and surprising. Conventional wisdom about secrecy and the use of in-space kinetic force to repel attacks gives way to more nuanced uses of informational methods (domain awareness), diplomatic approaches (norms of behavior), cyber intrusion, and the need for greater, more thoughtful, and universally known resilience methods as superior ways in which to resist attacks. Also of note is that, while the predominance of discussion around space attack seems to focus on what would be traditionally termed Phase 2 and 3 hostilities, the tools that might require more thought are those that can be employed below the level and before the start of all-out conflict, in the more ambiguous and less acute situations that are likely to be the rule rather than the exception in space conflict.¹

It is clear we are in the very early stages of developing the correct application of Sun Tzu's tenets to space combat. And since such conflict is unlikely to be a common occurrence in the foreseeable



future, thought pieces and exercises such as undertaken here will have an outsized role in that development. Additionally, the rate of technological change in this area is accelerating, and as mentioned earlier, that can turn well-understood operational concepts on their head if the underlying lessons are lost in the process of focusing on specific implementations.

In the interwar years between World War I and World War II, forward-thinking naval officers theorized and war-gamed the use of carrier-based and submarine-based naval power in exercises called “Fleet Problems” despite the dominant notion of the superiority of the battleship. Those “problems,” practiced and played out under the title of War Plan Orange, became the furnace in which operational experience could be forged—put crucially to the test after December 1941. Space needs the same forward-looking, innovative approach to examining strategic concepts—its own set of furnaces to forge its future strategy—before it has its own “space Pearl Harbor.” This study is one of the first—it won’t be the last.

Douglas L. Loverro, Colonel USAF (Ret)

*Former Deputy Assistant Secretary of
Defense for Space Policy*

“Harry wandered over to the
Restricted Section . . .

Unfortunately, you needed a
specially signed note from one of
the teachers to look in any of the
restricted books, and he knew
he’d never get one. These were
the books containing powerful
Dark Magic never taught at
Hogwarts, and only read by older
students studying advanced
Defense Against the Dark Arts.”

HARRY POTTER AND THE SORCERER’S STONE



SPACE IS NO SANCTUARY

The United States is increasingly dependent on space systems for economic and military security. The expansion of government and commercial space capabilities has opened markets and made possible whole new industries within the United States and around the world. Ride-sharing apps such as Uber and Lyft, the ultra-efficient supply chains of businesses, and the grocery delivery services many depended on during the Covid-19 pandemic would not be possible without the U.S. military-operated Global Positioning System (GPS). Moreover, the global economy depends not just on the weather, communications, navigation, timing, and remote sensing data from space systems but also on the global reach and power projection capabilities of U.S. and allied militaries that protect the global commons and the free flow of global commerce.

Space, however, is not a sanctuary. While this pronouncement has become somewhat cliché among policy analysts, the history behind this statement is often overlooked. Since the begin-

ning of the space age, when early satellites began to provide nascent military capabilities, nations started developing ways to deny others the military benefits of space. In 1959, just two years after the launch of Sputnik, the United States tested the first anti-satellite (ASAT) weapon—a Bold Orion missile launched from a B-47 bomber.² The Soviets soon followed, beginning tests of a space-based co-orbital ASAT weapon system in 1963 and declaring the system fully operational by 1973.³ Space was never really a sanctuary.

Although space was a contested domain from nearly the beginning, none of the kinetic ASAT weapons developed by the United States and the Soviet Union were ever used in conflict. While the threat of attack was ever present during the Cold War, a stable deterrence posture developed between the two superpowers because both U.S. and Soviet national security space systems were primarily used to support nuclear forces. Multiple agreements and treaties between the two nations formalized a mutual understanding

that an attack on these space systems would be regarded as a prelude to a nuclear attack. The foundation of deterrence in space was nuclear deterrence on Earth.⁴

What is different today is that the ability of the United States to deter attacks in space is in doubt. National security space systems are not just used to support nuclear forces, and the U.S. military is increasingly dependent on space systems across the full spectrum of military operations. Counterterrorism operations in the Middle East use drones enabled by GPS and satellite communications (SATCOM) systems to track and strike high-value targets. Space-based imagery, signals intelligence, and other surveillance systems provide real-time global monitoring of adversary forces that otherwise would not be possible. And nuclear forces stand watch day and night using many of the same satellites to quickly detect missile launches and ensure the national command authority remains connected before, during, and after a nuclear attack.

"Indifference and neglect often do much more damage than outright dislike."

ALBUS DUMBLEDORE,
HARRY POTTER AND THE
ORDER OF THE PHOENIX

Space provides an economic and military advantage to the United States that is not easily replicated by other nations or by capabilities in other domains. In the three decades since the end of the Cold War, adversaries have taken note of these advantages. Rather than fight the U.S. military symmetrically, they have invested heavily in counterspace weapons designed to degrade, disrupt, and destroy U.S. and allied space systems. These counterspace weapons can hold satellites at risk in a crisis and, in conflict, could greatly increase the risks to U.S. forces and interests around the world. As Chief of Space Operations General John Raymond has made clear, "space is a vital national interest and freedom of action must be preserved. No one wants a conflict in space and deterrence is a top priority . . . however, if deterrence fails, we must be prepared to fight and win."⁵

With the growing U.S. dependence on space and the proliferation of counterspace capabilities, the natural question for strategists and policymakers is how can space assets be protected against such threats? This report provides an overview of the range of protections that can be used to defend space systems from different forms of attack and the impact these defenses can have on deterrence and escalation dynamics. For space to remain a source of economic and military advantage, the United States must be able to defend its critical space infrastructure and have integrated space strategy, doctrine, and operational concepts for how to use these defenses across the full spectrum of conflict.

Space provides an economic and military advantage to the United States that is not easily replicated by other nations or by capabilities in other domains. In the three decades since the end of the Cold War, adversaries have taken

THE STATE OF SPACE TODAY

The current space environment is significantly different than it was during the Cold War. Space systems can no longer hide behind the cloak of nuclear deterrence, and the defenses needed for space systems must account for how the space environment is changing. Space is more diverse, disruptive, disordered, and dangerous than in the past. Space is more diverse because it is no longer dominated by the United States and Soviet Union. While 93 percent of all space launches during the Cold War were by the two superpowers, the majority of launches today are by other nations. Moreover, roughly 90 percent of satellites launched in 2020 were commercial rather than government.⁶ Space is more disruptive because many private companies are pursuing new space missions, such as on-orbit servicing of satellites and in-space mining and manufacturing. Other private firms are venturing into space missions that previously were the exclusive domain of

nation states, such as space-based radar and radio frequency (RF) monitoring. SpaceX, for example, has disrupted the launch market with its partially reusable Falcon 9 rocket and is now attempting to disrupt the communications market with its Starlink constellation of satellites. The Starlink constellation alone now has more operational satellites in orbit than China.⁷

These disruptions throw into sharp relief the increasingly disordered environment space has become. In many cases, national laws and regulatory frameworks do not fully account for some of the new commercial space missions being pursued. And with few legally binding or enforceable international treaties governing space, some nations and private entities are pushing the limits on what others may see as acceptable behavior in space. Space is also becoming increasingly dangerous as more nations develop and proliferate counterspace capabilities. Recent reports by CSIS, the Secure World Foundation, and the Defense Intelligence Agency provide an aggregation of publicly available information on the development, testing, and use of counterspace weapons by other nations.⁸ These reports show that while Russia and China continue to develop and test a wide range of counterspace weapons, even some friendly countries, such as India and France, are developing their own counterspace capabilities in response.

MILITARIZATION VERSUS WEAPONIZATION OF SPACE

The increased development and proliferation of counterspace weapons has led to a greater focus on space policy issues, specifically the militarization and weaponization of space. The term "militarization of space" is generally used to denote the passive use of space

"Always use the proper name for things. Fear of a name increases fear of the thing itself."

ALBUS DUMBLEDORE, HARRY POTTER AND THE SORCERER'S STONE

CLICK TO
FLY BACK TO
THE CONTENTS

systems to support military planning and operations on Earth. Space has been used for military purposes since the beginning of the space age, and it remains one of the main uses of space today. Militaries around the world use space systems for intelligence, surveillance, and reconnaissance (ISR); communications; position, navigation, and timing (PNT); and other functions to allow terrestrial forces to operate more effectively and efficiently. Space is already militarized and will remain militarized for the foreseeable future.

The weaponization of space, in contrast, is generally defined as going a step beyond the mere passive use of space for military purposes. In *Space as a Strategic Asset*, Dr. Joan Johnson-Freese notes that “force application is the overt weaponization of space, as compared with the de facto weaponization that has occurred under the guise of space control.”⁹ In 2004, U.S. Air Force doctrine defined space force application as “those forces that deliver kinetic effects to, from, or through space,” though this definition was removed from the Department of Defense’s (DoD) dictionary in 2018.¹⁰ The U.S. military defines space control to include both offensive and defensive operations that “ensure freedom of action in space for the US and its allies and, when directed, to deny an adversary freedom of action in space.”¹¹

A variety of other nations and international organizations have attempted to define what constitutes a space weapon, without much success in reaching a broad consensus. It is useful, however, to have a framework for understanding the types of systems that could potentially be considered space weapons. A prior CSIS report proposed such a framework for weapons that are either based in space or are designed to have effects in space.¹²

This framework, shown in



TABLE 1: FRAMEWORK FOR TYPES OF SPACE WEAPONS

	KINETIC	NON-KINETIC
EARTH-TO-SPACE	<p>EXAMPLE Direct-Ascent ASAT</p> <p>HOW DO THEY WORK? A missile fires a warhead or projectile into space to directly strike or detonate near a target satellite. The warhead can be conventional or nuclear.</p> <p>WHAT ARE THE EFFECTS? A kinetic Earth-to-space weapon produces space debris that can affect the safe operation of other satellites in affected orbits. Nuclear detonations in space increase the radiation exposure of other satellites and can significantly shorten their lifespan.</p> <p>HAVE THEY BEEN DEMONSTRATED? Earth-to-space kinetic weapons have been tested by the United States, Russia, China, and India. The United States and Soviet Union tested nuclear weapons in space in the 1960s.</p>	<p>EXAMPLES Uplink Jammer, Laser Dazzler/Blinder, Cyberattack</p> <p>HOW DO THEY WORK? Non-kinetic counterspace weapons can be stationed on ground, maritime, or airborne platforms and used to affect the operation of satellites or the sensors they carry, without making physical contact.</p> <p>WHAT ARE THE EFFECTS? Non-kinetic weapons disrupt or degrade the ability of satellites to function properly. They can have temporary or permanent effects, but they do not generally produce orbital debris or other collateral damage.</p> <p>HAVE THEY BEEN DEMONSTRATED? Multiple nations have demonstrated these capabilities, including Russia, China, Iran, and others.</p>
SPACE-TO-SPACE	<p>EXAMPLES Co-orbital ASAT, Space-Based Missile Defense Interceptors</p> <p>HOW DO THEY WORK? A satellite is placed into orbit and maneuvers to intercept its target by striking it directly or detonating a conventional or nuclear warhead in its vicinity.</p> <p>WHAT ARE THEIR EFFECTS? A kinetic space-to-space weapon would produce space debris that can affect the safe operation of other satellites in similar orbits. A nuclear detonation in space would increase the radiation exposure of other satellites and significantly shorten their lifespan.</p> <p>HAVE THEY BEEN DEMONSTRATED? The Soviet Union tested co-orbital kinetic ASAT weapons repeatedly during the Cold War.</p>	<p>EXAMPLES Co-orbital Crosslink Jammer, Co-orbital High-Powered Microwave</p> <p>HOW DO THEY WORK? A satellite is placed into orbit and uses non-kinetic means (such as a high-powered microwave or jammer) to disrupt the operation of another satellite.</p> <p>WHAT ARE THEIR EFFECTS? They can degrade, disrupt, or destroy a target satellite without making physical contact, producing orbital debris or otherwise affecting other satellites. The effects can be temporary or permanent depending on the form of attack used and the protections on the target satellite.</p> <p>HAVE THEY BEEN DEMONSTRATED? No open-source examples could be found of such a system being demonstrated, although such tests could look like remote proximity operations to outside observers.</p>
SPACE-TO-EARTH	<p>EXAMPLE Space-Based Global Strike (e.g., “Rods from God”)</p> <p>HOW DO THEY WORK? Weapons are placed in orbit and, when commanded, deorbit and reenter the atmosphere to strike a target on the Earth. Damage can be inflicted using the kinetic energy of the weapon itself, or a warhead can be deployed from the reentry vehicle (either conventional or nuclear).</p> <p>WHAT ARE THEIR EFFECTS? The effects depend greatly on the type of warhead used (conventional or nuclear) but would be like terrestrial-based ballistic missiles in terms of their ability to hit targets anywhere on Earth with little warning.</p> <p>HAVE THEY BEEN DEMONSTRATED? While the idea of using space-based weapons for prompt global strike has been contemplated by the U.S. military, there are no open-source examples of such a system being tested.</p>	<p>EXAMPLES Space-Based Downlink Jammer, Space-Based High-Powered Laser</p> <p>HOW DO THEY WORK? A satellite equipped with a non-kinetic weapon could target forces on Earth, such as a laser used to intercept missiles or aircraft in-flight or a jammer used to interfere with radars or satellite ground stations.</p> <p>WHAT ARE THEIR EFFECTS? When used, the effects would be localized to the target area, but such a system could theoretically strike anywhere without warning.</p> <p>HAVE THEY BEEN DEMONSTRATED? While the U.S. military has contemplated space-based lasers for boost-phase missile defense, there are no open-source examples of such a system being tested.</p>



gories of potential space weapons organized by the domain in which they originate and have effects (Earth-to-space, space-to-space, and space-to-Earth) and the means by which these effects are achieved (kinetic and non-kinetic). As noted in the table, other nations have already developed and tested three of the six categories of space weapons in the framework. Thus, by nearly any definition, space has already been weaponized.

SPACE ORGANIZATIONS

The organization of national security space capabilities by nations provides insight into how they view this domain from a security perspective. For example, the United States has long maintained a division between military space missions conducted by DoD and national intelligence space missions conducted mainly by the National Reconnaissance Office (NRO). Within the U.S. military, the organization of space forces recently changed with the re-establishment of United States Space Command (USSPACECOM) as a separate unified combatant command and the creation of the United States Space Force as a new military service. Like the other military services, the U.S. Space Force is responsible for organizing, training, and equipping space forces for the U.S. military.¹³ And like the other combatant commands, USSPACECOM is charged with using these space forces to carry out joint space missions and operations and support operations in other domains.¹⁴ This reorganization is itself a reflection of how the United States has changed its perception of the space domain and the threats posed by other nations in space.

Like the United States, countries such as China, Russia, France, Japan, and India have changed the way they organize their national security space capabilities. China's national security space organizations are part of the People's Liberation Army (PLA). Two divisions within the PLA focus on space and counterspace capabilities: the Strategic Support Force (SSF) and the PLA Rocket Force (PLARF). Created in 2015, the SSF is responsible for developing and employing China's military space systems as well as its cyber and electronic warfare systems. As one PLA officer noted, the SSF combines into one organization cyber forces for network attack and defense; space forces responsible for communications, reconnaissance, and navigation satellites; and electronic warfare units used for countering adversary radar and communications. This indicates that the PLA views the space domain as primarily an information domain and a key element of the PLA's information warfare forces.¹⁵

The primary space focus of China's SSF appears to be the development, launch, and operation of China's space-based command and control, PNT, and ISR capabilities. The SSF also appears to be leading the development and deployment of many Chinese counterspace capabilities, but it is unclear if all counterspace capabilities have been transferred to this organization. It is possible that Chinese direct-ascent ASAT weapons remain under the control of the PLA Rocket Force, which is also responsible for its missile programs.¹⁶ However, reports in 2019 indicated that the SSF began training with direct-ascent ASAT missiles capable of targeting satellites in low Earth orbit (LEO).¹⁷

The Russian Aerospace Forces are a military branch within the Russian Armed Forces focused on the air and space domains. A sub-branch within the Russian Aerospace Forces is the Russian Space Force, which is tasked with all military operations in the space domain, "including launching military satellites, maintaining space-based assets, monitoring space objects, and identifying potential attacks against the Russian homeland from space."¹⁸ Russian ASAT capabilities are scattered throughout the military, to include housing direct-ascent ASAT programs within the Russian missile forces and space-based co-orbital ASAT systems within the Russian Space Force.¹⁹

France has the world's third-oldest space program and a long history in space exploration. France's national space agency, Centre National d'Études Spatiales (CNES), manages all national civil space programs, and France is a key member in the European Space Agency (ESA). While CNES focuses on civil space programs, the French military contains separate space organizations for national security. France recently renamed the French Air Force to the French Air and Space Force and announced plans to create a Space Command within this newly renamed organization. France's recent *Space Defense Strategy*, released in 2019, calls for "renewed analysis of the space environment and its threats, risks and opportunities" and notes that threats in the space domain "force our country to revisit its model in order to remain a leading space power."²⁰

While Japan does not yet have significant military space capabilities, it is beginning to organize itself for military space operations. In 2019, Japan created its Space Domain Mission Unit, a military organization dedicated to protect-



ing Japanese space assets. The Space Domain Mission Unit will coordinate with Japan's civil space agency, the Japan Aerospace Exploration Agency (JAXA), and its U.S. counterparts in USSPACECOM and the U.S. Space Force. The Space Domain Mission Unit plans to be fully operational by 2022. Beyond space technology development and planning, the unit will be responsible for operating the satellite ground stations that are critical for Japan's self-defense missions. Reports also indicate that the Japanese government is considering investing in some combination of passive and active defenses to protect its space assets.²¹

In April 2019, shortly after conducting its first successful ASAT test, India established its Defence Space Agency (DSA). India's existing national security-focused space organizations—including the Defence Imagery Processing and Analysis Centre and the Defence Satellite Control Centre—will become a part of the DSA. The DSA's objective is to coordinate among the space assets of the Indian Air Force, Army, and Navy. Additionally, the DSA will be responsible for developing national security space assets and defending Indian space infrastructure through a new sub-organization entitled the Defense Space Research Organization.²²

REPORT ORGANIZATION AND METHODOLOGY

This report builds on prior work of the CSIS Aerospace Security Project and expands into several new areas. Chapter 2 provides a summary of the threats to space systems and a taxonomy for discussing different types of counterspace weapons. Chapter 3 catalogs the range of active and passive defenses that are theoretically possible and discusses the advantages and limitations of each. Chapter 4 analyzes how the defensive capabilities described in Chapter 3 can be applied to the different types of counterspace weapons discussed in Chapter 2. Chapter 5 explores a range of plausible scenarios in which defenses may be needed, concepts for employing different types of defenses, and how defensive actions in space may be perceived by others. The final chapter summarizes conclusions drawn from the analysis, actionable recommendations for policymakers, and additional research topics to be explored in future work.

"I solemnly swear that I am up to no good."
GEORGE WEASLEY, HARRY POTTER AND THE PRISONER OF AZKABAN

THE NEED FOR SPACE DEFENSES

The recent reorganization and elevation of national security space capabilities by each of the world's major space powers is an indication of the increasing importance these nations place on the use of space for military purposes. In many ways, the 2007 Chinese anti-satellite test served as a wake-up call for policymakers by highlighting the vulnerabilities of space systems. But since that time, improvements in the defenses of U.S. space systems to the types of counterspace weapons adversary nations are developing and operationally deploying has been slow and uneven. While U.S. space capabilities remain far ahead of other nations, some adversaries, namely China and Russia, are arguably making advances in counterspace weapons faster than the United States is making advances in protections against these threats.

Since the 2007 Chinese ASAT test, a variety of studies, exercises, and events have highlighted the vulnerabilities of space systems, the far-reaching effects of "a day without space," and the fact that space is a contested warfighting domain. However, the lack of public discourse about how to defend against space threats has led some to conclude that space is not defensible and should not be relied upon by the military, with one scholar writing that, "space is an inherently vulnerable and offense-dominant domain . . . There simply aren't many good options for space hardening/defenses." This scholar goes on to conclude that "the reality is that satellites are vulnerable to attack—through both kinetic and non-kinetic means from lasers, electronic warfare, and cyber—and there is no good way to fix this."²³

The fact that space is contested does not mean that space is undefendable. Rather, it means that the United States will have to fight to protect its ability to operate in this domain, just as it does in the air, land, and maritime domains. What is needed are strategy, doctrine, operational concepts, and technical capabilities that focus on protecting space systems, the services they provide, and the space environment itself.

Part of the methodology behind this study is the use of workshops with space and policy experts to test space crisis scenarios and operational concepts for space defenses. The CSIS study team developed several candidate scenarios, which are documented in Chapter 5, and presented them to a group of experts during two separate half-day online workshops in September 2020. The workshop participants were asked to explore the range of defensive space capabilities they would consider using given the situation described in each of the scenarios. The findings from these workshops were used to refine the scenarios themselves as well as the frame-

work of defenses in Chapter 3 and the concepts for employing defenses in Chapter 4.

The ultimate objective of this study is to facilitate debate among policymakers, technical experts, and the overall national security community on how best to defend space assets. This debate is especially important at this junction because the U.S. military is in the process of modernizing many of its key satellite constellations. The decisions made now about what types of space architectures to field and which defenses to incorporate will have repercussions for the life of these architectures. This report is intended to serve as a reference guide for understanding different forms of space defenses and how these defenses can be employed. While there is no easy or one-size-fits-all solution to defending U.S. space assets, the goal is to give decisionmakers the tools and information they need in an easily accessible format to have an informed policy debate about this complex and nuanced issue.



THE DARK ARTS IN SPACE

"The Dark Arts are many, varied, ever-changing and eternal. Fighting them is like fighting a many-headed monster, which, each time a neck is severed, sprouts a head even fiercer and cleverer than before. You are fighting that which is unfixed, mutating, indestructible."

SEVERUS SNAPE, HARRY POTTER AND THE HALF-BLOOD PRINCE

attack are direct-ascent ASAT weapons, co-orbital ASAT weapons, and ground station attacks. Direct-ascent ASAT weapons are launched on a sub-orbital trajectory to strike a satellite in orbit, while co-orbital ASAT weapons are first placed into orbit and then later maneuvered into their intended target. Attacks on ground stations are targeted at the terrestrial sites responsible for command and control of satellites or the relay of satellite mission data to users.

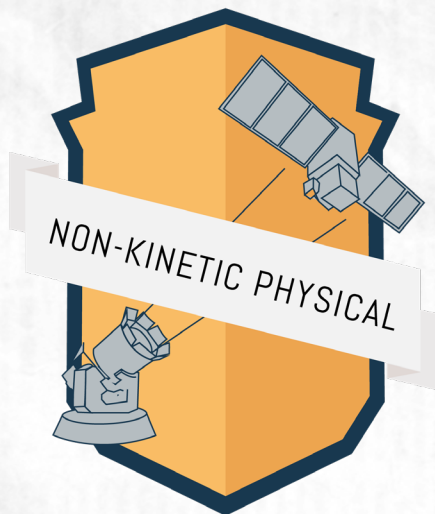
Kinetic physical attacks tend to cause irreversible damage to the systems affected and demonstrate a strong show of force that would likely be attributable and publicly visible. A successful kinetic physical attack in space will produce orbital debris, which can indiscriminately affect other satellites in similar orbits. These types of attacks are one of the only counterspace actions that carries the potential for the loss of human life if targeted at crewed ground stations or at satellites in orbits where humans are present, such as the International Space Station in LEO. To date, no country has conduct-

A prerequisite to understanding space defenses is understanding what they are intended to defend against. This chapter provides an overview and taxonomy for counterspace weapons. The high stakes at play in the space domain have incentivized nations to build arsenals of counterspace weapons to disrupt, degrade, or destroy space systems. Counterspace weapons vary significantly in the types of effects they create, how they are deployed, how easy they are to detect and attribute, and the level of technology and resources needed to develop and field them. They can be categorized into four broad groups of capabilities: kinetic physical, non-kinetic physical, electronic, and cyber.



Kinetic physical counterspace weapons attempt to strike directly or detonate a warhead near a satellite or ground station. The three main types of kinetic physical forms of

ed a kinetic physical attack against another country's satellite, but four countries—the United States, Russia, China, and India—have successfully tested kinetic physical counterspace weapons.



Non-kinetic physical counterspace weapons have physical effects on satellites or ground systems without making physical contact. Lasers can be used to temporarily dazzle or permanently blind the sensors on satellites, and higher-powered lasers can cause components to overheat. High-powered microwave (HPM) weapons can disrupt a satellite's electronics or cause permanent damage to electrical circuits and processors in a satellite. A nuclear device detonated in space can create a high radiation environment that has indiscriminate effects on satellites in all affected orbits. These attacks operate at the speed of light and, in some cases, can be less visible to third-party observers and more difficult to attribute.²⁴

Satellites can be targeted with lasers and HPM weapons from ground- or ship-based sites, airborne platforms, or other satellites. A satellite lasing system requires high beam quality, adaptive optics (if being used through

the atmosphere), and advanced pointing control to steer the laser beam precisely—technology that is costly and requires a high degree of sophistication. An HPM weapon can be used to disrupt a satellite's electronics, corrupt data stored in memory, cause processors to restart, and, at higher power levels, cause permanent damage to electrical circuits and processors. A laser can be effective against a sensor on a satellite if it is within the field of view of the sensor, making it possible to attribute the attack to its approximate geographical origin. HPM attacks can be more difficult to attribute because the attack can come from a variety of angles, including from other satellites passing by in orbit. For both laser and HPM weapons, the attacker may have limited ability to know if the attack was successful because it is not likely to produce visible indicators.²⁵

The use of a nuclear weapon in space would have large-scale, indiscriminate effects that would be attributable and publicly visible. A nuclear detonation in space would immediately affect satellites within range of its electromagnetic pulse, and it would also create a high radiation environment that would accelerate the degradation of satellite components over the long term for unshielded satellites in the affected orbital regime. The detonation of nuclear weapons in space is banned under the Partial Test Ban Treaty of 1963, which has more than 100 signatories, although China and North Korea are not included.²⁶

Among U.S. competitors, China and Russia appear to have the most developed non-kinetic physical ASAT capabilities. For example, China has been working on a satellite lasing system since at least 2006 when it illuminated a U.S. government satellite flying over Chinese territory without causing any

known damage.²⁷ For its part, Russia has continued to develop its non-kinetic ASAT capabilities in recent years, including by conducting research on nano-sized aerosol obscurants that can be used in space to block RF or optical transmissions and placing satellite lasing systems on aircraft and ground vehicles.²⁸



Electronic counterspace weapons target the electromagnetic spectrum through which space systems transmit and receive data. Jamming devices interfere with the communications to or from satellites by generating noise in the same radio frequency band. An uplink jammer interferes with the signal going from Earth to a satellite, such as the command-and-control uplink. Downlink jammers target the signal from a satellite as it propagates down to users on the Earth. Spoofing is a form of electronic attack where the attacker tricks a receiver into believing a fake signal, produced by the attacker, is the real signal it is trying to receive. A spoofer can be used to inject false information into a data stream or, in extremis, to issue false commands to a satellite to disrupt its operations. User terminals with omnidirectional antennas, such as many GPS receivers and satellite



phones, have a wider field of view and thus are susceptible to downlink jamming and spoofing from a wider range of angles on the ground.²⁹

Electronic forms of attack can be difficult to detect or distinguish from accidental interference, making attribution and awareness more difficult. Both jamming and spoofing are reversible forms of attack because once they are turned off, communications can return to normal. Through a type of spoofing called “meaconing,” even encrypted military GPS signals can be spoofed. Meaconing does not require cracking the GPS encryption because it merely rebroadcasts a time-delayed copy of the original signal without decrypting it or altering the data.³⁰ The technology needed to jam and spoof many types of satellite signals is commercially available and inexpensive, making them relatively easy to proliferate among state and non-state actors.

While Russia and China have advanced electronic counterspace capabilities, nations such as Iran and North Korea are also developing and using jamming and spoofing systems. North Korea likely acquired much of its electronic counterspace systems from Russia, and it appears to be gaining operational experience using these systems in peacetime. For example, it frequently uses GPS jamming to interfere with U.S.-South Korean military exercises and disrupt air and maritime traffic along the border with South Korea.³¹ Likewise, the U.S. Department of Transportation issued a warning in 2019 about Iranian GPS jamming and communications spoofing in the Strait of Hormuz. Iran is believed to have placed GPS jammers on an island near the entrance to the strait to interfere with civilian aircraft and ships so that they might mistakenly navigate into Iranian waters or airspace and could be seized.³²



While electronic forms of attack attempt to interfere with the transmission of RF signals, cyberattacks target the data itself and the systems that use, transmit, and control the flow of data. Cyberattacks on satellites can be used to monitor data traffic patterns, intercept data, or insert false or corrupted data in a system. These attacks can target ground stations, end-user equipment, or the satellites themselves. While cyberattacks require a high degree of understanding of the systems being targeted, they do not necessarily require significant resources to conduct. The barrier to entry is relatively low, and cyberattacks can be contracted out to private groups or individuals. Even if a state or non-state actor lacks internal cyber capabilities, it may still pose a cyber threat.

A cyberattack on space systems can result in the loss of data or services being provided by a satellite, which could have widespread systemic effects if used against a system such as GPS. Cyberattacks could have permanent effects if, for example, an adversary seizes control of a satellite through its command-and-control system. An attacker could shut down all communications and permanently damage the satellite by expending its propellant supply or

issuing commands that would damage its electronics and sensors. Accurate and timely attribution of a cyberattack can be difficult because attackers can use a variety of methods to conceal their identity, such as using hijacked servers to launch an attack.

China has been implicated or suspected in several cyberattacks against U.S. satellites. In October 2007 and again in July 2008, China is suspected of attacking a remote sensing satellite operated by the U.S. Geological Survey called *Landsat-7*, causing more than 12 minutes of interference with ground station control each time.³³ In June and October 2008, hackers also believed to be from China attacked NASA’s Earth observation satellite, *Terra*, and this time they “achieved all steps required to command the satellite but did not issue commands.”³⁴ And in September 2014, Chinese hackers attacked the National Oceanographic and Atmospheric Administration’s (NOAA) satellite information and weather systems, forcing NOAA to take down the system and stop transmitting satellite images to the National Weather Service for two days.³⁵



SPACE

DEFENSES DEFINED

DEFENSIVE COUNTERSPACE OPERATIONS

Given the wide range of threats and the proliferation of counterspace capabilities outlined in the previous chapter, the United States and others are necessarily placing a greater focus on the ability to identify threats and defend space systems from attack. In 2018, the Joint Chiefs of Staff published an update to its space operations doctrine, the first update since 2013, which noted that:

Whereas earlier space operations integration efforts focused primarily on providing capability from space to support

*terrestrial forces, the focus now includes the equally demanding and more complex task of assuring and defending our space capabilities against the aggressive space activities of others.*³⁶

While the inclusion of defensive space operations in joint doctrine is an important start, much work remains to be done to develop the operational concepts and technical capabilities necessary to make defensive counterspace operations credible and effective. Existing space doctrine and planning guidance state that the objective of defensive counterspace operations is to protect friendly space systems from “attack, interference, and unintentional hazards” and that these operations can occur “before, during, or after an attack.”³⁷ Friendly space systems can include civil, commercial, and foreign

“Your defences must therefore be as flexible and inventive as the arts you seek to undo.”

SEVERUS SNAPE, HARRY POTTER AND THE HALF-BLOOD PRINCE

military systems that the United States or its allies rely upon. In contrast, the objective of offensive counterspace operations is to prevent an adversary’s use of space capabilities and counterspace weapons to threaten friendly forces or support its own forces on Earth.³⁸ These operations can include reversible or irreversible attacks against an adversary’s satellites, ground control systems, communication links, or the space services provided by third parties.

In general, defensive counterspace operations aim to protect friendly space systems, while offensive counterspace operations aim to disrupt, degrade, or destroy adversary space systems. A gray area that can be interpreted as either defensive or offensive, depending on one’s perspective, is when one nation’s counterspace capabilities are used to attack an adversary’s counterspace capabilities. French minister of armed forces Florence Parly provided an example of this in a speech announcing the nation’s new *Space Defense Strategy* in 2019: “If our satellites are threatened, we will consider dazzling those of our opponents. We reserve the time and means of the response: this may involve the use of high-power lasers deployed from our satellites or from our patrol nano-satellites.” She went on to make the case that this use of coun-

terspace operations is not offensive, noting that “active defence is not an offensive strategy, what it is about is self-defence. It is, when a hostile act has been detected, characterized and attributed, able to respond in an appropriate and proportionate manner, in accordance with the principles of international law.”³⁹ Moreover, U.S. military joint doctrine on space operations states that “active measures to deceive, degrade, or destroy targeting systems are examples of defensive operations.”⁴⁰ But to neutral third-party observers that do not have access to the same intelligence as the nations in conflict, a defensive counterspace attack may be indistinguishable from an offensive counterspace attack. This is especially true in a pre-conflict environment where one nation may feel compelled to act preemptively or before evidence of an attack has been disclosed.

Due to the unique physics of this operating environment and that space remains an asymmetric advantage for the United States, actions that are likely to result in orbital debris or trigger an adversary response that would result in orbital debris can disproportionately and adversely affect the United States, its allies and partners, and their collective long-term economic and security interests in space. The United States and its allies and partners therefore have an incentive to avoid using kinetic defensive counterspace capabilities that are likely to produce orbital debris if possible.

This chapter provides an overview of options available to protect space systems from attacks, including each of the four categories of counterspace weapons discussed in the previous chapter. While the following is not an exhaustive list of defensive capabilities, it is intended to provide an overview of the range of options available

and the strengths and weaknesses of each. Importantly, many of the defenses discussed can be used in parallel with one another to enhance overall protection of space systems. Where

possible, examples are used to highlight existing space systems that employ these defenses, although in some cases examples may not exist or may not be publicly disclosed.

PASSIVE DEFENSES

Passive counterspace defenses are measures that can be used to minimize the effectiveness of attacks on friendly space systems by making them harder to target or better capable of withstanding attacks. The passive defenses discussed in this section are divided into three rough categories—architectural, technical, and operational—although it should be noted that some passive defenses could arguably belong in more than one category. Architectural defenses are those that rely primarily on satellite constellation and ground station architectures that are more difficult for an adversary to attack. Technical defenses rely primarily on technologies that can be incorporated into satellites, ground stations, and user equipment that makes the system more difficult to attack. Operational defenses rely primarily on changes in the way satellites are operated to make them more difficult to target, more resistant to attacks, or easier to restore after an attack.

ARCHITECTURAL DEFENSES

Disaggregated Constellations

Disaggregation is the separation of distinct missions onto different platforms or payloads, effectively breaking up multi-mission satellites into separate mission-specific satellites that operate in parallel.⁴¹ For example, the U.S. Space Force currently plans to separate the strategic and tactical protected SATCOM missions into two separate next-generation systems. The Evolved Strategic SATCOM (ESS) system will support strategic users for missions such as nuclear command and control, whereas the Protected Tactical Service (PTS) system will support tactical SATCOM users that need a high level of jam resistance.⁴² This could reduce the potential for unintentional escalation by forcing an adversary to be explicit about the capabilities it is targeting in an attack.⁴³

In a conventional conflict, if an adversary targets a dual-use (strategic and tactical) aggregated space system such as the current Advanced EHF system, it may not be clear whether the strategic or tactical missions (or both) are the intended target. This could lead to miscalculations and unintentional escalation. If the strategic and tactical payloads are disaggregated into separate space systems, an adversary could target the tactical system only and leave the strategic system unharmed if it does not want to risk nuclear escalation. However, an adversary may not be able to distinguish between satellites that are intended for different missions, and even if such differences are disclosed, an adversary may not trust this distinction and attack both anyway. Moreover, disaggregation of strategic and tactical missions may make attacking the tactical system in a conventional conflict more attractive if the risk of strategic escalation is reduced.



Disaggregation can reduce space system complexity and potentially speed acquisition timelines by decoupling requirements.⁴⁴ However, disaggregated systems can cost more in total because separate space systems must be developed and launched, resulting in some redundancies in development, testing, production, and launch costs.

Distributed Constellations

A distributed system uses “a number of nodes, working together, to perform the same mission or functions as a single node.”⁴⁵ In a distributed constellation, the end user is not dependent on any single satellite but rather uses multiple satel-

“We are only as strong as we are united, as weak as we are divided.”

ALBUS DUMBLEDORE,
HARRY POTTER AND
THE GOBLET OF FIRE

ellites to derive a capability. A distributed constellation can complicate an adversary’s counterspace planning by presenting a larger number of targets that must be successfully attacked to achieve the same effects as targeting just one or two satellites in a less-distributed architecture.⁴⁶ GPS is an example of a distributed constellation because the functioning of the system is not dependent on any single satellite or ground station; a user can use any four satellites within view to get a time and position fix. SpaceX’s Starlink constellation is a commercial example of a distributed architecture because it uses more than 1,000 satellites circling in LEO to provide continuous coverage over large parts of the Earth, with users of the system automatically being transferred between satellites as they pass in and out of range. Distributed constellations tend to degrade gracefully as satellites are removed from the system, gradually reducing the accuracy, coverage, and time availability of the service.⁴⁷

Distributed constellations can use dedicated satellites that are smaller and less

complex because they do not have to provide an entire capability on one platform. They can also use hosted payloads on other types of satellites, which can have the benefit of further complicating targeting for an adversary by forcing it to attack multiple satellites, potentially from multiple countries and commercial firms, rather than a single nation’s military satellite. However, hosted payloads can also result in more aggregated architectures since the host satellite may be supporting multiple payloads and missions.

Proliferated Constellations

Proliferated satellite constellations deploy a larger number of the same types of satellites to similar orbits to perform the same missions.



While distribution relies on placing more satellites or payloads on orbit that work together to provide a complete capability, proliferation is simply building more systems (or maintaining more on-orbit spares) to increase the constellation size and overall capacity.⁴⁸ Proliferation can be an expensive option if the systems being proliferated are individually expensive, although highly proliferated systems may reduce unit costs in production from the learning curve effect and economies of scale.⁴⁹ The U.S. military’s Wideband Global SATCOM (WGS) system is an example of a proliferated system, with a constellation that has grown from three “gapfiller” satellites initially to a planned constellation of 11 satellites.⁵⁰ The Space Development Agency is planning to develop highly proliferated constellations for data transport, missile warning, missile tracking, and alternative position, navigation, and timing that would use hundreds of satellites in LEO.⁵¹ Proliferated systems can provide a greater degree of protection because they increase the number of satellites an adversary must successfully attack

to achieve the same effects as targeting a smaller number of satellites in a less-proliferated architecture.

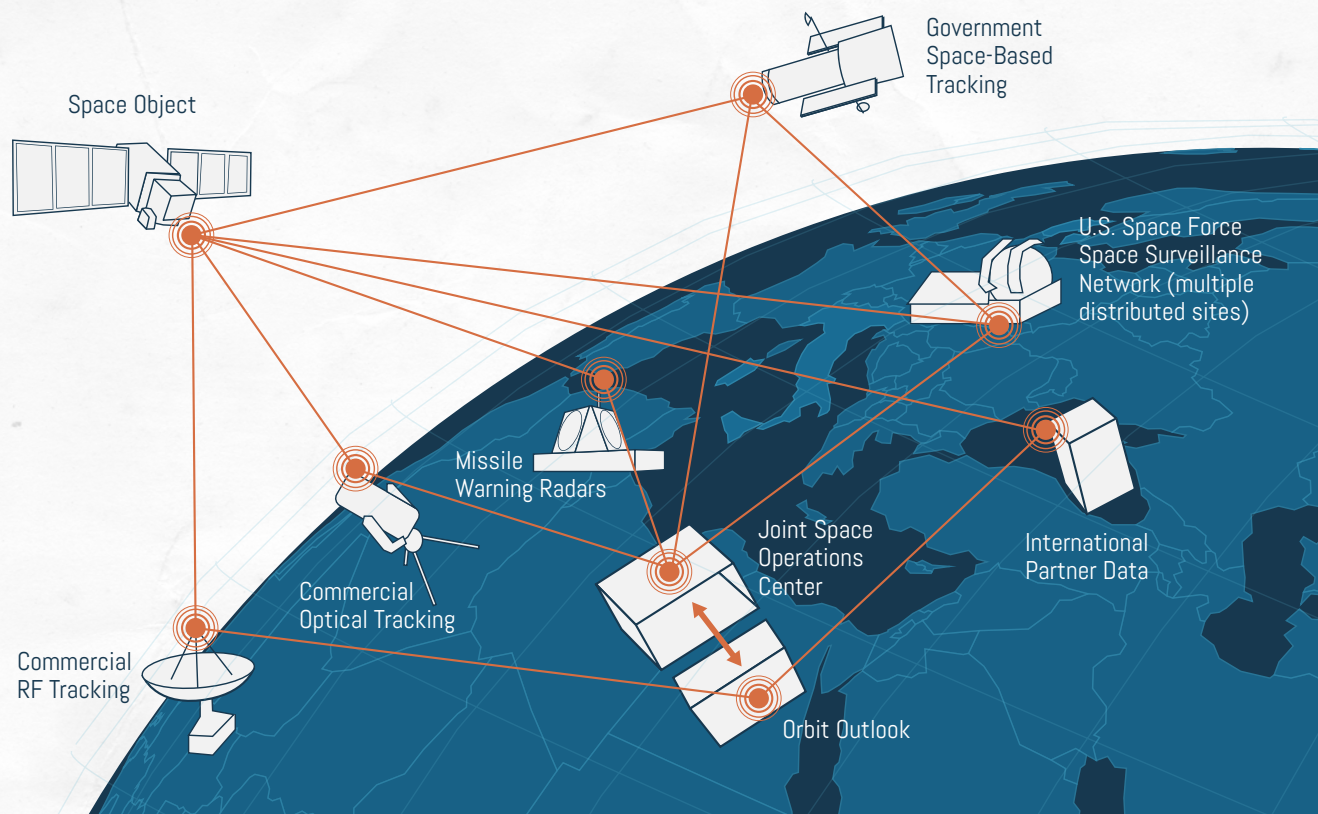
Diversified Architectures

In a diversified architecture, multiple systems contribute to the same mission using platforms and payloads that may be operating in different orbits or in different domains.⁵² For example, wideband communications to fixed and mobile users can be provided by the military’s WGS system, commercial SATCOM systems, airborne communication nodes, or terrestrial networks. The Chinese BeiDou system for positioning, navigation, and timing uses a diverse set of orbits, with satellites in geostationary orbit (GEO), highly inclined GEO, and medium Earth orbit (MEO).⁵³ Diversification reduces the incentive for an adversary to attack any one of these systems because the impact on the overall mission will be muted since systems in other orbits or domains can be used to compensate for losses. Moreover, attacking space systems in diversified orbits may require different capabilities for each orbital regime, and the collateral damage from such attacks, such as orbital debris, could have a much broader impact politically and economically.

Redundant, Mobile, or Hardened Ground Stations

Ground stations used for command and control of a satellite or for the operation of the payloads on a satellite are also at risk of attack. Having redundant or rapidly deployable mobile ground stations provides a measure of protection in the event of attack or natural disaster, making the space system less dependent on any single ground station or location.⁵⁴ Ground stations can also be hardened to withstand kinetic and non-kinetic attacks on the facilities themselves and the local infrastructure on which they depend.





Example Space Domain Awareness (SDA) Network.

TECHNICAL DEFENSES

Exquisite Space Domain Awareness

The credibility and effectiveness of many other types of defenses are enabled or enhanced by the ability to quickly detect, characterize, and attribute attacks against space systems. Space domain awareness (SDA) includes identifying and tracking space objects, predicting where objects will be in the future, monitoring the space environment and space weather, and characterizing the capabilities of space objects and how they are being used.⁵⁵ Exquisite SDA—information that is more timely, precise, and comprehensive than what is publicly available—can help distinguish between accidental and intentional actions in space. As U.S. Space Force Major General Leah Lauderback noted in public comments, “it’s difficult trying to characterize what happens thousands of miles away, all

through technical means,” and the military needs capabilities that allow it to “make a more confident call in a faster manner.”⁵⁶

Improved SDA can cut through the “fog of war” by providing an information and decisionmaking advantage over adversaries. For example, being able to track, identify, and characterize objects in space is critical to identifying that an attack is in progress and mounting an effective defense against threats such as co-orbital kinetic ASAT weapons and space-based electronic attack. Artificial intelligence (AI) can further enhance SDA capabilities by tracking patterns of life in space to better identify abnormal or nefarious behaviors that human analysts may miss. AI can also potentially be used to better understand satellite capabilities, including covert capabilities, based on how these satellites are maneuvered

“The truth . . . it is a beautiful and terrible thing, and should therefore be treated with great caution.”

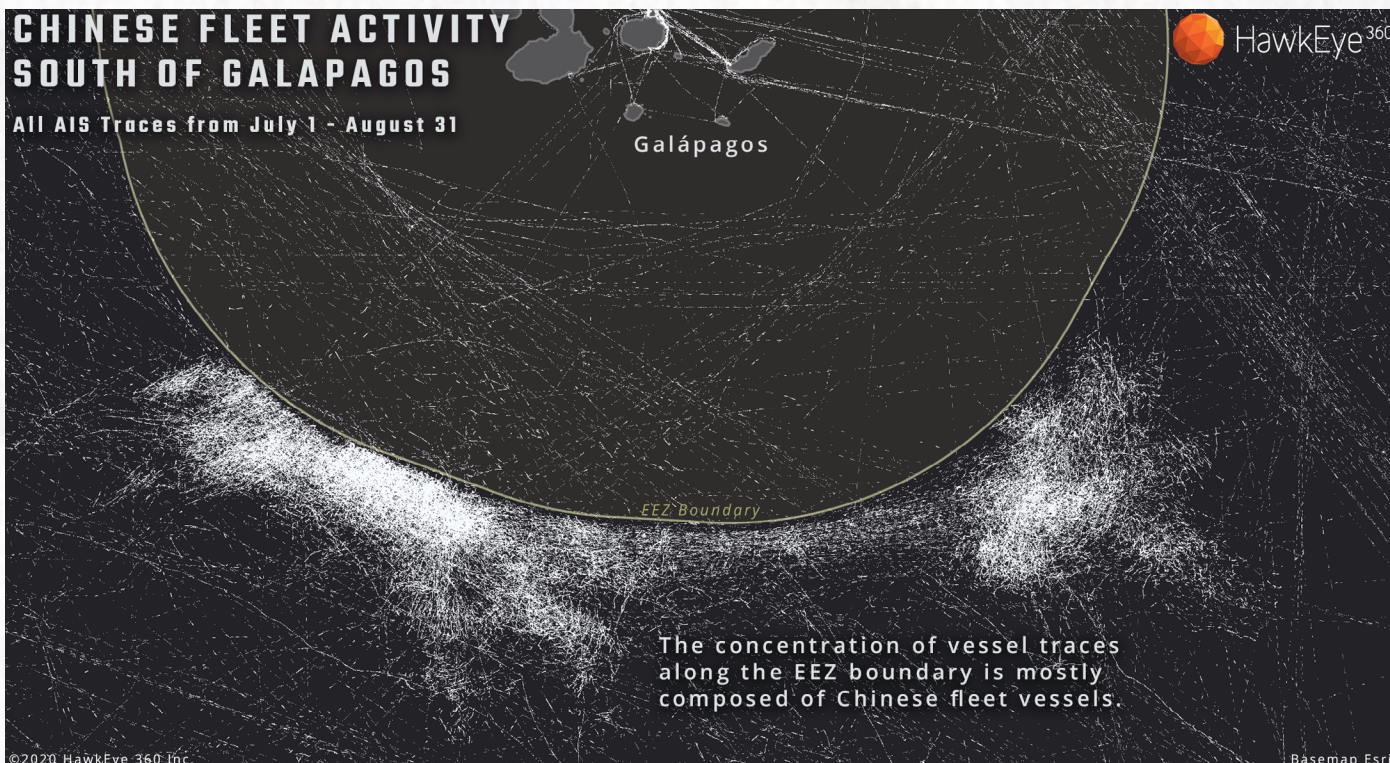
ALBUS DUMBLEDORE,
HARRY POTTER AND THE
SORCERER’S STONE

and operated. Moreover, if one’s SDA capabilities can be communicated publicly and some of the data can be released when necessary, the mere existence of these capabilities can be a deterrent in some situations by providing greater attribution and public visibility into adversary space activities.



SDA systems include terrestrial-based optical, infrared, and radar systems as well as space-based sensors, such as the U.S. military’s Geosynchronous Space Situational Awareness Program (GSSAP) inspector satellites.⁵⁷ Many nations have SDA systems with various levels of capability, and an increasing number of private companies (and amateur space trackers) are developing their own space surveillance systems, making the space environment more transparent to all users.⁵⁸





Radio frequency mapping of the Galapagos Islands in 2020.

HAWKEYE360

Space-Based Radio Frequency Mapping

Space-based RF mapping is the ability to monitor and analyze the RF environment that affects space systems both in space and on Earth. Similar to exquisite SDA, space-based RF mapping provides space operators with a more complete picture of the space environment, the ability to quickly distinguish between intentional and unintentional interference, and the ability to detect and geolocate electronic attacks. RF mapping can allow operators to better characterize jamming and spoofing attacks from Earth or from other satellites so that other defenses can be more effectively employed.

Without timely data, it can be difficult to distinguish between accidental and intentional RF interference. For example, the U.S. military experienced an average of 23 satellite communications jamming incidents per month in 2015, and

the cause was “almost always self-jamming.”⁵⁹ Commercial firms can play a role in RF mapping and determining the sources of interference. For example, the private firm HawkEye360 is launching a constellation of satellites that can detect and geolocate RF transmissions.⁶⁰ A key aspect of RF mapping is timeliness—the faster a threat can be detected, identified, and characterized, the more valuable this information becomes as an enabler for other defensive capabilities. And like exquisite SDA data, the ability to release information publicly or privately on the sources, locations, and nature of jamming incidents can act as a deterrent to adversaries that would prefer to operate covertly or in a more ambiguous or less attributable manner.

Electromagnetic Shielding

Satellite components can be vulnerable to the effects of background radiation in the space environment and de-

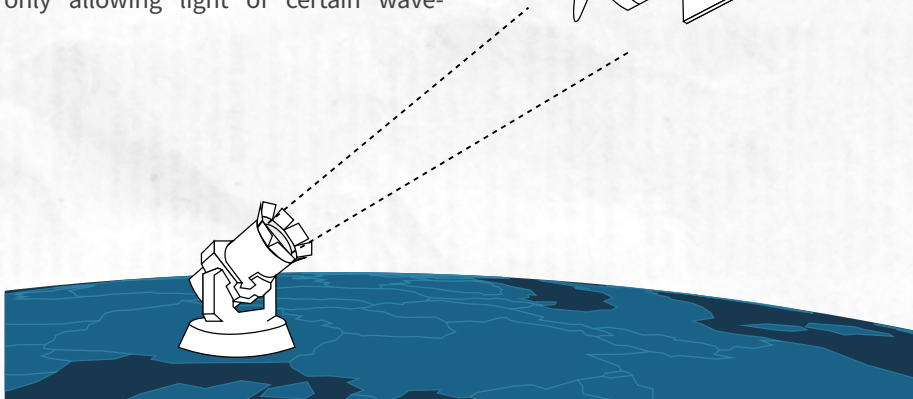
liberate attacks from HPM and electromagnetic pulse weapons. The effects can include data corruption on memory chips, processor resets, and short circuits that permanently damage components. One of the first instances of an on-orbit failure due to these effects was the *Telstar-1* satellite in 1962, which succumbed to the intensified radiation environment in space created by a U.S. high-altitude nuclear test.⁶¹ Surrounding the electronics and cables within a satellite with shielding and adding surge protection devices throughout the RF and electrical system can protect against the effects of radiation, high-powered microwave attacks, and electromagnetic pulse weapons. However, these protections add weight and complexity to satellites, and the effectiveness of shielding depends on precise manufacturing processes that must be carefully and laboriously tested and validated.

CLICK TO
FLY BACK TO
THE CONTENTS



Filtering and Shuttering

Filters and shutters can be used on remote sensing satellites to protect sensors from laser dazzling and blinding. Filters can protect sensors by only allowing light of certain wave-



Shuttering against lasing attack.

lengths to reach the sensors. Filters are not very effective against lasers operating at the same wavelengths of light the sensors are designed to detect because a filter that blocks these wavelengths would also block the sensor from its intended mission. A shutter acts by quickly blocking or diverting all light to a sensor once an anomaly is detected or a threshold is reached, which can limit damage but also temporarily interrupts the collection of data.⁶² Filters and shutters add weight and complexity to satellite designs and may require a detailed understanding of the technical capabilities of adversary counterspace weapons.

Jam-Resistant Waveforms

The way data is encoded for transmission on a radio wave (i.e., the waveform) is a key factor in how difficult that transmission is to jam or spoof. Different types of waveforms can be used to improve the resistance of communications systems to jamming and spoofing, such as using frequency hopping spread spectrum (FHSS) and interleaving.⁶³ FHSS involves rapidly changing the transmission frequency using a pseudorandom pattern. This protects against jamming by making

it difficult for a jammer to match the frequency of transmission. By spreading the signal across a larger piece of spectrum, the signal also has “processing gain” that allows it to effectively boost the signal-to-noise ratio and better withstand jamming.⁶⁴ The power level of a spread spectrum signal can also be lower, making it harder for an adversary to detect or intercept without knowing the precise hopping pattern.

Interleaving is the process of dividing and mixing the bits of data being transmitted in a noncontiguous manner. Because RF interference tends to occur in



bursts, errors often occur in adjacent bits of data in transmission. If more bit errors occur in a

data packet than the error correction algorithm can accommodate, the data packet becomes corrupted. Interleaving reduces this risk by shuffling the order of the data before it is transmitted and then reassembling it in proper order when it is received but before the error correction algorithm is applied. This reduces the chance that a burst of interference will create multiple errors within a single data packet.⁶⁵

While these techniques can make communications more difficult to jam, they do not make them completely jam-proof. For example, a high-powered wideband jammer can interfere with signals across a larger portion of the spectrum used for frequency hopping, which increases the odds that some of the frequencies in the hopping pattern will be jammed, especially if the jammer is near the receiver. Interleaving also adds latency in communications because it takes longer for the shuffled data to be reassembled into the original data packets on the receiving end.

Antenna Nulling and Adaptive Filtering



Satellites can be designed with antennas that “null” or minimize signals from a particular geographic region on the surface of the Earth or locations in space where jamming is detected.⁶⁶ Nulling is useful when jamming is from a limited number of detectable locations, but one of the downsides is that it can also block trans-

ORIGINAL MESSAGE:

A	A	A	A	B	B	B	B	C	C	C	C	D	D	D	D	E	E	E	E	F	F	F	F	G	G	G	G
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

INTERLEAVED MESSAGE:

A	B	C	D	E	F	G	A	B	C	D	E	F	G	A	B	C	D	E	F	G	A	B	C	D	E	F	G
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

INTERLEAVED MESSAGE WITH BURST ERROR:

A	B	C	D	E	F	G	A	B	C	D	E	F	G	A	B	C	D	E	F	G	A	B	C	D	E	F	G
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

RECEIVED MESSAGE AFTER DEINTERLEAVING:

A	B	C	D	E	F	G	A	B	C	D	E	F	G	A	B	C	D	E	F	G	A	B	C	D	E	F	G
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

missions from friendly users that fall within the nulled area. If a jammer is sufficiently close to friendly forces, the nulling antenna may not be able to block the jammer without also blocking legitimate users.

Adaptive filtering, in contrast, is used to block specific frequency bands regardless of where these transmissions originate. Adaptive filtering is useful when jamming is consistently within a particular range of frequencies because these frequencies can be filtered out of the signal received on the satellite while transmissions can continue around them. However, a wideband jammer could interfere with a large enough portion of the spectrum being used that filtering out the jammed frequencies would degrade overall system performance.

Encryption and Air-Gapped Systems

While the encryption of data transmissions for the command and control of national security space systems is standard practice, this is not always the case for commercial operators and international partners. The RF transmissions to and from satellites are inherently exposed and need strong encryption as well as some of the jam resistance techniques discussed previously. The ground systems used to process and disseminate data on other networks can also be a vector for cyberattacks. Air-gapped systems that are physically separated from the public internet can make attempts to infiltrate a system much more difficult for an adversary without insider help. However, it is not always possible to completely air-gap some space systems because the data they produce may be intended for public consumption, such as data from weather satellites or satellites that are intended for commercial use.



A risk with encryption is that the encryption keys could be compromised through the loss of sensitive hardware or software. The systems therefore need to be capable of being rapidly and securely rekeyed. An additional risk is that a previously unknown flaw in the encryption algorithm could be exploited by an adversary. Quantum computing, for example, could pose a risk to many existing encryption methods because the higher processing speed of these systems could allow for a brute-force attack that cracks the encryption key, leading researchers to push for the development of quantum-proof encryption.⁶⁷

OPERATIONAL DEFENSES

Rapid Deployment

Rapid deployment is a form of protection that involves the speedy launch of a new or expanded space capability when needed. Keeping a capability on the ground until needed can protect the system from pre-emptive attack and limit an adversary's knowledge of the system and ability to factor it into strategic planning. Such a system would need to be developed, tested, and procured well in advance of need so that the satellites and necessary ground systems are ready for launch and initial operations. Space operators would also need sufficient training and simulations to understand how to operate the system and take advantage of the capabilities it provides.

The speed at which a new satellite can be launched is limited by several factors, including the availability of a suitable launch vehicle; the time required to integrate the satellite with the launch vehicle; the time needed to prepare the vehicle for launch; the availability of a launch window to the desired

orbit; and the weather and other potential range safety hazards that can delay launch plans. Air-launched systems can help broaden the range of launch windows available and potentially fly around weather or other range obstructions, but the time required to integrate a satellite with a launch vehicle and prepare the vehicle for launch are likely to remain limiting factors. Moreover, satellites and ground station components procured for rapid deployment will become technologically obsolete over time and will need to be replaced periodically even if they are never used.

Reconstitution

Reconstitution can be used to quickly replace existing space capabilities by launching more satellites or bringing online more ground stations “to restore functionality to an acceptable level for a particular mission, operation, or contingency after severe degradation.”⁶⁸ Replacement satellites either of a different design or copies of the operational satellites on orbit can be built in advance and stored on the ground in a clean room or other controlled environment to be ready for launch when needed. Similarly, mobile ground stations can be deployed or existing ground stations can be brought online or repurposed to replace sites that have been damaged or destroyed. These actions would allow the military to reconstitute space capabilities that have been degraded or destroyed, and it is one of the approaches

to space defense specifically mentioned in the 2018 *National Defense Strategy*.⁶⁹

Many of the limitations for how quickly a satellite can be launched discussed in the rapid deployment option would apply to reconstitution as well, namely the availability and integration with a suitable launch vehicle and the weather, range,

“Time will not slow down when something unpleasant lies ahead.”

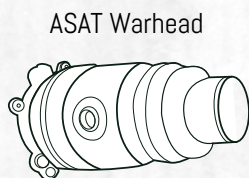
HARRY POTTER,
HARRY POTTER
AND THE GOBLET
OF FIRE



and launch window constraints of the launch. However, speed may not be a major factor in reconstitution because an adversary could attack the replacement satellites or ground stations as long as it retains its counterspace capabilities. This could force the military to delay launching reconstitution satellites until it is confident that an adversary's counterspace capabilities have been sufficiently degraded, which may not be until near the end of major combat operations. Reconstitution systems would need to be tested and refreshed periodically as they age and become technologically obsolete regardless of whether they are launched.

Maneuver

Satellite maneuver is an operational tactic that can be used by satellites fitted with chemical thrusters to avoid kinetic and some directed energy ASAT weapons. For unguided projectiles, a satellite can be commanded to move out of their trajectory to avoid impact. If the threat is a guided projectile, like most direct-ascent ASAT and co-orbital ASAT weapons, maneuver becomes more difficult and is only likely to be effective if the satellite can move beyond the view of the onboard sensors on the guided warhead.⁷⁰ Maneuver also depends on having near-real-time and continuous tracking data for incoming warheads. Thus, maneuver is best employed in combination with other active defenses that target the sensors guiding an ASAT war-



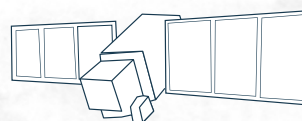
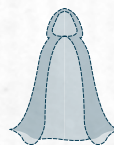
ASAT Warhead

head so that it cannot easily find a satellite once it has maneuvered.

Maneuvering a satellite quickly comes at the price of disrupting its current operations and using propellant reserves to maneuver out of position and then back into a useful orbit. The amount of propellant required for a maneuver increases significantly with the mass of the satellite and the speed of maneuver required. Maneuver can only be done a limited number of times, depending on the propellant available, and could ultimately reduce the useful lifetime of the satellite if the propellant needed for routine station keeping is expended prematurely.⁷¹ Guided ASAT warheads have a significant maneuver advantage because they are smaller, can accelerate faster using less propellant, and can afford to expend all their propellant since they are by definition expendable.⁷²

Stealth

Space systems can be operated and designed in ways that make them difficult to detect and track. Similar to platforms in other domains, stealthy satellites can use a smaller size, radar-absorbing coatings, radar-deflecting shapes, radar jamming and spoofing, unexpected or optimized maneuvers, and careful control of



Satellite maneuvers out a warhead's field of view.

reflected radar, optical, and infrared energy to make themselves more difficult to detect and track. For example, academic research has shown that routine spacecraft maneuvers can be optimized to avoid detection by known sensors.⁷³ Adding stealthy characteristics to satellites requires design trade-offs in terms of size, weight, and power, and it imposes some operational limitations on how the satellite can be used. And like stealthy platforms in other domains, no satellite can be perfectly stealthy all of the time, in all parts of the spectrum, and from all angles. It can also be difficult to know if a satellite has been discovered if others are using passive sensors to track the satellite, such as optical telescopes.

Deception and Decoys

Deception can be used to conceal or mislead others on the "location, capability, operational status, mission type, and/or robustness" of a satellite.⁷⁴ Public messaging, such as launch announcements, can limit information or actively spread disinformation about the capabilities of a satellite, and satellites can be operated in ways that conceal some of their capabilities. Another form of deception could be changing the capabilities or payloads on satellites while in orbit. Satellites with swappable payload modules could have on-orbit servicing vehicles that periodically move payloads from one satellite to another, further complicating the targeting calculus for an adversary because they may not be sure which type of payload is currently on which satellite.



Satellites can also use tactical decoys to confuse the sensors on ASAT weapons and SDA systems. A satellite decoy can consist of an inflatable device designed to mimic the size and radar signature of a satellite, and multiple decoys can be stored on the satellite for deployment when needed. Electro-



magnetic decoys can also be used in space that mimic the RF signature of a satellite, similar to aircraft that use airborne decoys, such as the ADM-160 Miniature Air-launched Decoy (MALD).⁷⁵ Decoys have been an important component of operations in other domains,

including the use of inflatable tanks during the Cold War to make armored units appear larger to an adversary.⁷⁶ Decoys can be more effective when used in combination with other defenses, such as stealth, maneuver, and electronic attack.

Requirements to satellites, competing for resources with their mission payloads. An off-board jamming and spoofing system could be placed on dedicated protective satellites that orbit near a satellite, roam among satellites as needed, or position themselves strategically to protect multiple satellites at once. A challenge for off-board systems is that they may not be within the field of view of the sensors on an incoming ASAT warhead when and where they are needed. For both onboard and off-board systems, their effective operation depends to a certain extent on an accurate characterization and understanding of the technical capabilities of the radar and communication systems on threats before an attack commences.

Laser Dazzling or Blinding

Laser systems can be used to dazzle or blind the optical or infrared sensors on an incoming ASAT weapon in the terminal phase of flight. This is similar to the laser infra-

ACTIVE DEFENSES

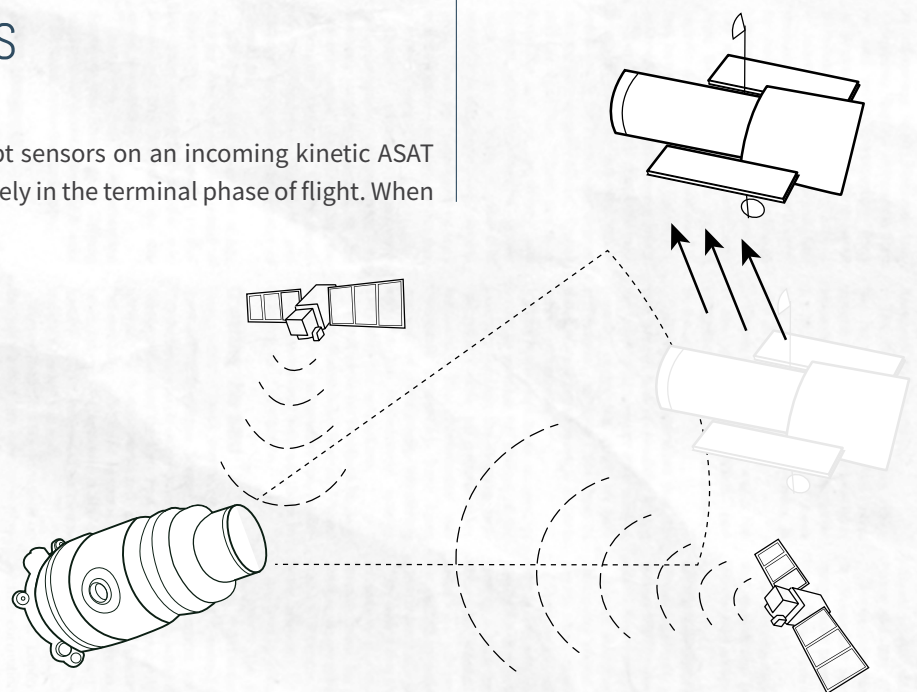
While passive defenses seek to protect space systems from threats by making them harder to target or better capable of withstanding attacks, active defenses target the threats themselves. As U.S. Space Force doctrine notes, active defenses are intended to “destroy, nullify, or reduce the effectiveness of threats holding friendly space capabilities at risk. Although this may entail reactive operations after an adversary has initiated an attack, active defense also includes proactive efforts to seize the initiative once an attack is imminent.”⁷⁷ Active defenses can be divided into two broad categories based on where these defensive systems are based. Space-based defenses include onboard systems that are integrated into the satellites they protect and off-board systems that are hosted on separate satellites. Off-board defenses can be used to provide “zone defense” of multiple satellites or to act as defensive patrols that roam within orbital regimes in response to threats. Terrestrial defenses are cross-domain systems based on Earth that target counterspace systems and the systems that support them either on Earth or in space.⁷⁸



SPACE-BASED DEFENSES

Jamming and Spoofing

A jammer or spoofer can be used to disrupt sensors on an incoming kinetic ASAT weapon so that it cannot steer itself effectively in the terminal phase of flight. When used in conjunction with maneuver, this could allow a satellite to effectively “dodge” a kinetic attack. Similar systems could also be used to deceive SDA sensors by altering the reflected radar signal to change the location, velocity, and number of satellites detected, much like digital radio frequency memory (DRFM) jammers used on many military aircraft today. A space-based jammer can also be used to disrupt an adversary’s ability to communicate with an ASAT weapon.



Bodyguard satellites jam the sensors on an incoming warhead while the target satellite maneuvers to safety.

An onboard jamming and spoofing system would add weight and power re-



red countermeasures used on aircraft to defeat heat-seeking missiles.⁷⁹ Blinding an ASAT weapon's guidance system and then maneuvering to a new position (if necessary) could allow a satellite to effectively "dodge" a kinetic attack. It could also be used to dazzle or blind the optical sensors on inspector satellites to prevent them from imaging a satellite that wants to keep its capabilities concealed or to frustrate adversary SDA efforts.

Onboard laser systems would add weight and power requirements to satellites, which would compete for resources with mission payloads. An off-board lasing system could be installed on dedicated protective satellites, provided these satellites are maneuvered within the field of view of the sensors of an incoming ASAT weapon when and where they are needed. Like space-based jamming and spoofing defenses, the effective operation of a space-based laser defense system depends on an accurate characterization and understanding of the technical capabilities of threats, such as the wavelengths of light to which adversary sensors are sensitive. France has publicly indicated that it intends to field a self-defense laser system to dazzle adversary satellites if one of its satellites is threatened.⁸⁰

Shoot-Back



Satellites can be equipped with systems that either fire a physical projectile at an incoming ASAT weapon or use a high-powered laser or microwave system to have physically destructive effects, such as overheating or causing short circuits, on an incoming ASAT weapon. The number of shots would be limited by the number of physical projectiles that could be stored on the satellite or the power capacity of the satellite to generate the large amounts of energy needed for successive high-powered laser or microwave bursts. A draw-

back to using a shoot-back system, particularly kinetic shoot-back, is that if it successfully strikes an incoming ASAT warhead, it could leave orbital debris that affects the safe operation of other satellites in similar orbits.

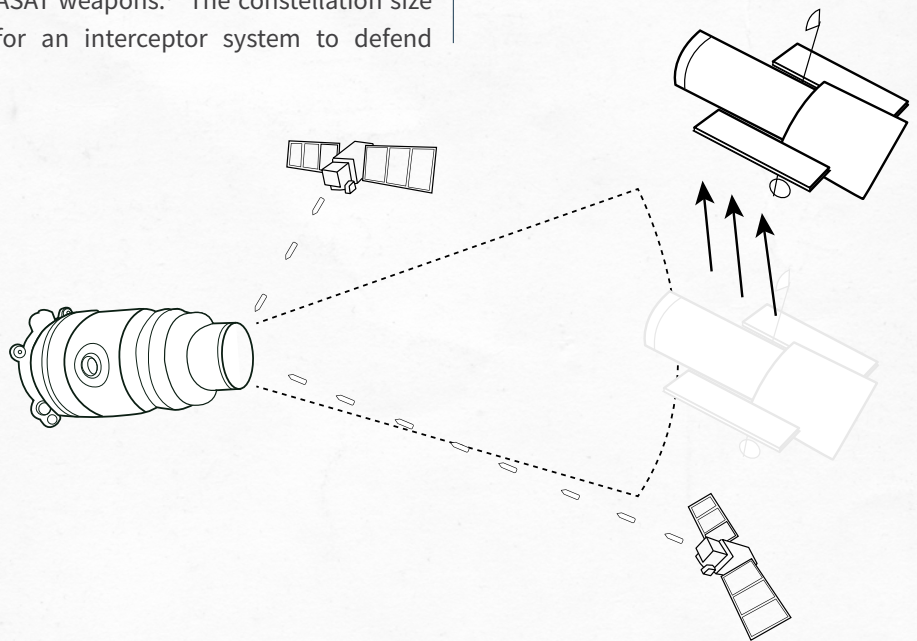
A shoot-back system can either be located on the satellite it is intended to defend or on a protective satellite in a similar orbit. An off-board shoot-back system could potentially protect many satellites in a distributed "zone defense" approach. A variation on this would be a co-orbital ASAT weapon that, instead of firing a projectile or directed energy weapon, uses the satellite itself as a warhead to strike a threat. An off-board shoot-back or co-orbital system would be similar in some ways to a space-based missile interceptor constellation, and one constellation could in theory be used for both missile defense and space defense. A potential weakness in this approach is that an adversary could launch a salvo of ASAT weapons or decoys to saturate defenses in a local area, creating a hole in the protective layer that could then be exploited by other ASAT weapons.⁸¹ The constellation size for an interceptor system to defend

against a salvo attack grows much faster than the number of missiles in the salvo, meaning that the attacker has a cost-imposing advantage at scale.⁸²

Physical Seizure



A space vehicle capable of docking with, manipulating, or maneuvering other satellites or pieces of debris can be used to thwart space-based attacks or mitigate the effects after an attack has occurred. Such a system could be used to physically seize a threatening satellite that is being used to attack or endanger other satellites or to capture a satellite that has been disabled or hijacked for nefarious purposes. Such a system could also be used to collect and dispose of harmful orbital debris resulting from an attack. A key limitation of a physical seizure system is that each satellite would be time- and propellant-limited depending on the orbit in which it is stored. A system stored in GEO, for example, would not be well positioned to capture an object in LEO because of the amount of propellant re-



Bodyguard satellites fire projectiles at an incoming warhead while the target satellite maneuvers to safety.



quired to maneuver into position. Physical seizure satellites may need to be stored on Earth and deployed once they are needed to a specific orbit to counter a specific threat.

While several commercial companies are developing capabilities for on-orbit servicing, a distinguishing feature of a military defensive capability is the ability to conduct remote proximity and docking operations with an uncooperative or uncontrolled space object. For example, the Northrop Grumman Mission Extension Vehicle (MEV) on-orbit serving satellites can attach themselves to a cooperative host satellite. They use their propulsion systems to maneuver the host satellite to a new orbit and take over station keeping—maintaining position in a desired orbit—for the remainder of the satellite's life.⁸³ Docking with an uncooperative satellite—either without the operator's consent or where control has been lost—is more difficult because the satellite could make unexpected movements, may be tumbling out of control, or may react to the docking in unexpected ways if its automatic control system remains engaged. Docking with a satellite under these conditions may require more

advanced capabilities, such as a robotic arm, harpoon, deployable net, or other device. Several countries and private companies are currently developing and testing active debris removal systems that could, in theory, be adapted for military uses.⁸⁴

TERRESTRIAL-BASED DEFENSES

Cyberattacks

Many forms of counterspace weapons rely on terrestrial systems for command and control or for targeting information derived from SDA networks. These terrestrial systems and the data networks that connect them can be targeted using cyberattacks to degrade adversary space battle management systems. Cyberattacks on ground control systems can include denial of service attacks; infiltration of systems for intelligence, data corruption, and sabotage; or seizure of command and control. These attacks can be used to achieve effects such as disrupting communications between counterspace forces and higher echelons of command; preventing commands from being sent to ASAT weapons in space; covertly degrading or corrupting SDA data; and taking control of

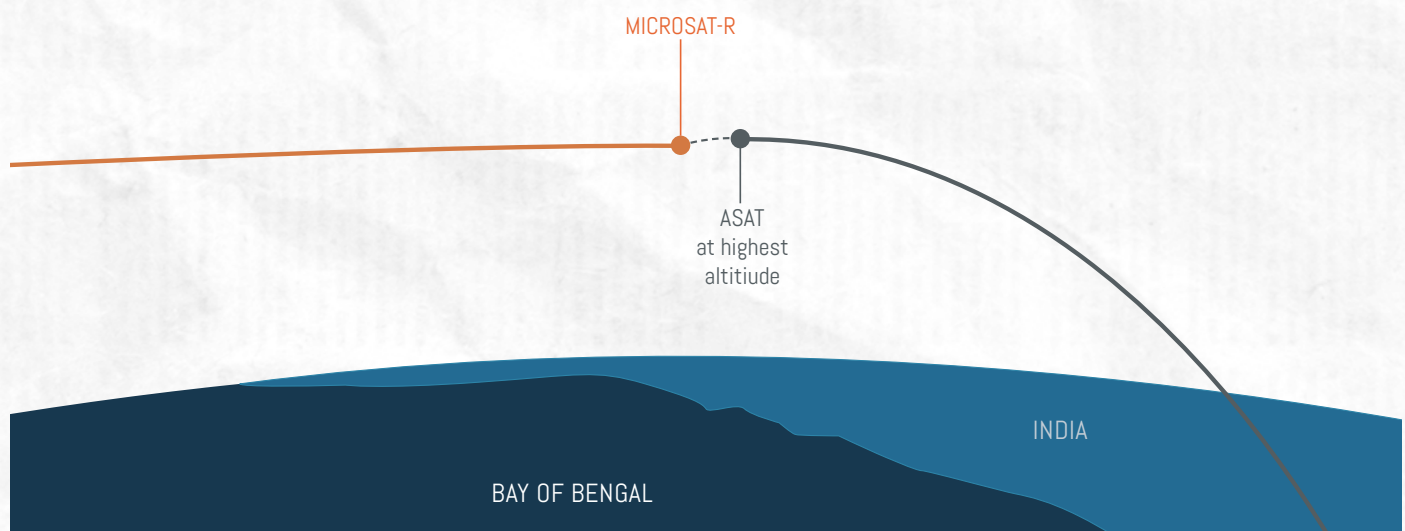
adversary space or counterspace systems. As with other types of cyberattacks, attribution can be difficult to determine with certainty, the effectiveness of cyber weapons may not be known until they are used, and the weaknesses a cyber weapon exploits may become known and mitigated once it is used.

Jamming and Spoofing

Terrestrial systems can also be used to jam or spoof uplink communications to counterspace weapons in space. If the system is dependent on ground commands for its operations, this could prevent an adversary from sending commands to the weapon. However, for jamming or spoofing of the uplink to be effective, the jammer or spoofer needs to be within the field of view of the antenna on the space system that receives the uplink. This form of defense may not be effective if the adversary counterspace system can carry out its mission autonomously or if it has alternative means of communications, such as using other satellites as communications relays.

Direct-Ascent ASAT

Direct-ascent ASAT weapons can be used in a defensive counterspace role



Indian direct-ascent ASAT test in March 2019.

to neutralize threatening objects in space. For example, if a satellite begins maneuvering in a dangerous or erratic manner or begins interfering with critical military space systems, a direct-ascent ASAT weapon could be used to physically destroy the threatening satellite before, during, or after an attack. However, this would create orbital debris which itself could pose a threat to other space systems. Moreover, this could be viewed by others as an offensive and escalatory act if the information justifying this action is not publicly available and credible.



Air-, Sea-, and Land-Based Kinetic Attacks

Kinetic attacks can be launched against adversary space and counterspace infrastructure in other domains to prevent attacks in space and to disable the terrestrial sites from which counterspace attacks are controlled. Targets for terrestrial kinetic attacks could include command and control facilities, missile and rocket launch sites, jamming and spoofing sites, and SDA facilities. It could also include attacks against key supporting infrastructure that space ground segment facilities depend upon, such as power systems, communications lines, and the industrial base that supports space and counterspace operations.



SPACE

DEFENSES APPLIED

Three fundamental questions arise when determining how to apply space defenses in a conflict. The first question is *if* defenses should be employed at all. Using defenses can expose capabilities, tactics, and thresholds for employment that an adversary can use to its advantage in further engagements. In cases of minor threats or attacks that are reversible and have low consequences, the best response may be no response. On the other hand, a lack of response may set precedent, lead to unfavorable norms for what is acceptable behavior, and constrain future decisions about whether a response is warranted.

A second question is *which* systems should be defended and the relative priorities among them. The U.S. military depends on many commercial and allied space systems as well as U.S. government space systems, and some of these

dependencies are more critical than others. Space defenses could be extended to non-U.S. government systems to help reassure allies and commercial firms in a crisis and deter threats. However, it could also lead to the United States being drawn in to intervene in a situation that it otherwise might want to avoid.

A third key question is *how* space systems should be defended in terms of the

actions and capabilities that are suitable for a particular situation. While the first two questions of *if* and *which* are mainly questions of strategy, the question of *how* is more a matter of technology and tactics. How to apply space defenses against counterspace weapons depends on many factors, including the type of counterspace weapons being used and the objectives of both the attacker and the defender—what they hope to achieve or deny the other side.

This chapter explores a range of objectives the attacker and defender each may have in a conflict that begins or extends into space and the suitability of different types of space defenses in pursuing or foiling these objectives. The focus in this discussion is on the space objectives in a conflict, which are a subset of the overall objectives each side may have. Importantly, both the attacker and defender may have multiple objectives in space, and these objectives may evolve over the course of a conflict. As objectives change, the desirability of different types of space defenses will also shift. This chapter closes with a summary table showing the potential application of the types of space defense capabilities discussed in Chapter 3 to the types of counterspace threats discussed in Chapter 2.

OBJECTIVES OF THE ATTACKER IN SPACE

For the foreseeable future, conflict in space will ultimately be about achieving economic and political effects on the ground—just as it is in the air and maritime domains.⁸⁵ But nations may

make the decision to begin or extend a conflict into space for many reasons. For the purposes of this discussion, the attacker is the actor that initiates the part of a conflict that extends to space. The objectives of an attacker in initiating conflict in space can include, but are not limited to: inflicting economic harm, signaling re-



solve, disrupting sensor-to-shooter kill chains, disabling adversary defenses in other domains, and permanently shifting the balance of power in space. While many other objectives are possible and an attacker can have multiple objectives simultaneously, these five represent a broad range of objectives that are possible and serve to illustrate how different forms of attack may be preferred depending on the attacker's objectives.

Attacks in space can be used to inflict economic harm or to disrupt commerce for strategic purposes by interfering with the space systems that commerce depends upon, such as GPS, weather satellites, and commercial satellite communications systems. For example, an attacker could use jamming of the civilian GPS signals to disrupt financial transactions, transportation systems, and the many other commercial activities that depend on GPS navigation and timing services. While terrestrial and airborne jammers can only affect the local region in which they operate, a space-based GPS jammer could affect much broader areas far beyond an attacker's terrestrial reach. If the intent is to inflict broad economic harm, the attacker may prefer to use forms of attack where attribution is more difficult to limit diplomatic backlash, such as cyberattacks against space systems.

A nation may also want to use attacks in space—or the threat of attacks—to signal resolve and to deter an opponent in a crisis. A limited and reversible attack in space or an ASAT test could be used by an attacker to demonstrate that it is willing and able to extend conflict into space. An attacker's ability to hold critical space systems at risk could affect the calculus of an opponent about whether to intervene in a conflict on Earth. Intervention by an opponent could be more costly in terms of

the forces and time required, and it could be riskier in terms of personnel losses, platform losses, and collateral damage if its space capabilities are degraded. For signaling and deterrence, an attacker may prefer to use forms of attack that are reversible and have low potential for collateral damage in space, such as electronic attacks, to give the other side an incentive and ability to deescalate. The method of attack would also need to be attributable because if the opponent does not know who is attacking its space systems, it may not be deterred or understand what the attack is intended to signal.

During or at the outset of a conflict, a nation may use attacks in space to disrupt the sensor-to-shooter kill chain of its opponent, making it more difficult for an opponent to conduct offensive operations in other domains. The sensor-to-shooter kill chain is the battle network that transports intelligence, targeting, and battle damage assessment information from sensors in various domains to nodes in the network that can process and analyze this information. This data is then used to make decisions and communicate those decisions to platforms and personnel that can direct fires accordingly.⁸⁶ Modern battle networks are increasingly complex, and many nodes and communication links in the kill chain can run through or be dependent on space—even if the sensor and shooter reside on the same platform. For example, the MQ-9 Reaper, a type of drone used extensively in the Iraq and Afghanistan wars, uses GPS for navigation, satellite communications for sending back video and other intelligence collected in real time, and control links through satellites so that operators can issue commands to the platform. Space is ideal for supporting kill chains that must extend over long distances, across multiple regions, or into regions

with limited terrestrial infrastructure. For these reasons, as nations seek to project power over longer distances, they may become increasingly reliant on space-based remote sensing and communications to close the sensor-to-shooter kill chain. If the intent of the attacker is to disrupt an adversary's kill chains, it may prefer methods of attack, such as kinetic physical counter-space weapons, where it can reliably determine if the attack was effective and whether the effects will be sustained throughout the conflict.

Attacks in space can also be used as a penetration aid for offensive strikes in other domains. For example, attacks against an opponent's missile warning or missile tracking satellites could be used to degrade its missile defense capabilities and improve the odds that a missile attack succeeds.⁸⁷ For this type of objective, the attacker may prefer to use kinetic physical attacks or cyberattacks so that it can quickly determine if its efforts were effective at disabling its opponent's defenses before it launches offensive attacks in other domains.

In a more extreme scenario, an attacker's objectives may include permanently altering the balance of power in space in its favor. This objective differs from the others previously described because the intent of the attacks is to have permanent disabling effects on the opponent's space systems that extend well beyond the current conflict. For example, this objective may include significantly degrading an opponent's space capabilities so that it can no longer support existing satellites or launch new satellites. It could include cyberattacks that cause permanent damage to satellites, large-scale kinetic physical attacks, or a nuclear detonation in space. The latter two examples could leave some orbital regimes unusable for all nations—a “clear the skies” approach.



OBJECTIVES OF THE DEFENDER IN SPACE

The way one defends against an attack in space depends in part on what the defender is trying to achieve or prevent. As in the case of an attacker, a defender's main concern in a conflict that begins or extends into space will likely remain rooted on the ground for the foreseeable future. But a nation may have a variety of objectives when it comes to how it chooses to defend its space capabilities. For the purposes of this discussion, the defender is defined as the actor that is the target of a potential attack in space. The objectives of a defender can include but are not limited to: deterring conflict in space, buying time for operations in other domains to succeed, defeating an attack and restoring the status quo in space, and permanently degrading an adversary's space and counterspace capabilities. Many other variations or combinations of these objectives are possible, but these four represent a broad range of objectives that elucidate how different types of defenses may be preferred depending on what a defender hopes to accomplish.



One of the main objectives in building space defenses can be deterrence. An opponent may be deterred from extending a conflict into space if space systems are less vulnerable and the opponent believes it is not likely to achieve its objectives through counterspace attacks. Improved defenses for some space systems could incentivize an opponent to attack less protected systems in space or in other domains. An opponent is likely to be deterred when the expected costs of a successful attack exceed the expected benefits. Space defenses can both raise the expected costs and reduce the expected benefits of beginning or extending conflict into space. But for space defenses to act as a deterrent, an opponent must believe that such defenses exist and that they are effective—even if the opponent does not fully understand what they are or how effective they may be. Defenses that rely on secrecy and that cannot be revealed without compromising their operation, such as stealth or the rapid deployment of previously undisclosed capabilities, are not likely to contribute effectively to deterrence. Some architectural defenses, such as distributed or proliferated constellations, raise the costs of attacking because many more satellites must be targeted, increasing the time and number of weapons required and the risks of collateral damage and escalation. Diversified systems, many types of technical defenses, demonstrated ability to reconstitute, and some active defenses can reduce an attacker's expected benefits for different forms of attack by making their counterspace weapons less effective.

Another objective for space defenses can be to buy time for operations in other domains to be effective in determining the outcome of a conflict. For this objective, the defender will want to focus on limiting disruptions and degradation in space services (i.e., space domain mission assurance) as long as possible and may be willing to accept some losses if they occur gradually.⁸⁸ The defender could use this time to mount offensive attacks in other domains, which could themselves be dependent on space capabilities. If the objective is to buy time and weather an attack, the de-

fender may prefer space capabilities that degrade gracefully, such as distributed and diversified architectures, and many types of passive technical defenses that make systems more resistant to attacks. The defender may want a reconstitution capability to replace systems during a conflict even if the replacements may also be lost. It may also be desirable to have a rapid deployment capability to bring new capabilities online during the conflict that an adversary may not be expecting, to further complicate its targeting calculus and supplement systems that are being degraded.

The defender's objective could also be to defeat an attack and quickly restore space capabilities to full operations. For example, a defender could attempt to seize the initiative once an attack extends into space by quickly degrading the counterspace capabilities of the attacker to limit or halt any further attacks, potentially using offensive actions for defensive purposes. In addition to the defensive capabilities previously discussed that are preferred to buy time in a conflict, a space counterattack could also require a mix of active defenses, such as non-kinetic space-based shoot-back systems and terrestrial kinetic attacks, to target an adversary's counterspace weapons directly. Returning space systems to full operations may also require a reconstitution capability to replace systems that experienced permanent damage, but reconstitution operations would likely not begin until the attacker's counterspace capabilities are neutralized. Kinetic space-based shoot-back systems may not be desirable because orbital debris could make a return to the status quo in space more difficult if not impossible.

A more ambitious objective for a defender is to permanently shift the balance of power in space, ensuring that when a conflict subsides the aggressor



is no longer a threat. To do this, a defender would need to defeat an attack once it has begun and then work to roll back and possibly eliminate the counterspace capabilities of the attacker. This objective may also include degrading the space capabilities of the attacker if these space capabilities could pose a threat on Earth or in space. For this objective, the defender will likely place more emphasis on active defenses, technical defenses (e.g., exquisite SDA) that enable these defenses, and defenses that have permanent disabling effects on an adversary's counterspace capabilities.

MATCHING DEFENSES TO THREATS

The best defense to use against an attack in space depends not just on the objectives of the attacker and defender but also on the specific types of weapons being used. Jam-resistant waveforms, for example, can help protect against electronic forms of attack but are of no value when defending against a direct-ascent ASAT weapon. Similarly, active defenses such as an on-orbit shoot-back system can be effective against kinetic physical forms of attack but would not be useful against an airborne lasing system.

Another complicating factor in space, which arises in the cyber domain and in the use of remotely piloted aircraft, is that proportionality, including when certain defensive measures are warranted, can be difficult to ascertain when human lives are not directly at risk. Proportionality is highly dependent on the context of a situation, and that context can be difficult to understand in a timely manner in a remote environment such as space. At present, all military space systems are remotely operated and an attack on a satellite does not risk the direct loss of human life, with few exceptions. But some of the defensive options available, particularly kinetic attacks on terrestrial counterspace facilities, could put humans lives at risk. It is difficult to weigh proportionality when the risks for one side involve loss of property or critical infrastructure and the risks for the other side involve loss of life.
















































It can also be difficult to discern the intent of an attack in space from the effects created. For example, a defender may not be able to tell if a lasing event that blinded an imagery satellite was only intended to temporarily dazzle its sensors. And it may not be clear if an attack against a satellite used for both nuclear and conventional missions is a prelude to nuclear escalation. Policymakers therefore need a range of defensive options available to provide decision space as a crisis evolves rather than singular or formulaic solutions.

The following table is a crosswalk between the different types of defenses discussed in Chapter 3 and the different categories of threats presented in Chapter 2. It provides a brief description of the desired effects from each type of defensive capability (if it is used successfully) and indicates the categories of threats for which it is potentially applicable. Importantly, a particular type of defense may only be applicable to a subset of the threats possible within a given category. For example, filtering and shuttering would help protect an imagery satellite against laser dazzling and blinding, but it would not protect against other types of non-kinetic physical threats, such as high-powered microwave weapons.

CLICK TO
FLY BACK TO
THE CONTENTS



TABLE 2: APPLICATION OF SPACE DEFENSES TO TYPES OF COUNTERSPACE WEAPONS

TYPES OF DEFENSES		DESIRED EFFECTS	POTENTIALLY APPLICABLE TO:
PASSIVE DEFENSES	ARCHITECTURAL	Disaggregated Constellations	   
		Distributed Constellations	  
		Proliferated Constellations	  
		Diversified Architectures	   
		Redundant, Mobile, or Hardened Ground Stations	 
	TECHNICAL	Exquisite Space Domain Awareness	  
		Space-Based Radio Frequency Mapping	 
		Electromagnetic Shielding	
		Filtering and Shuttering	
		Jam-Resistant Waveforms	
		Antenna Nulling and Adaptive Filtering	
		Encryption and Air-Gapped Systems	 
	OPERATIONAL	Rapid Deployment	   
		Reconstitution	  
		Maneuver	
		Stealth	  
		Deception and Decoys	  
ACTIVE DEFENSES	SPACE-BASED	Jamming and Spoofing	 
		Laser Dazzling/Blinding	 
		Shoot-Back	 
		Physical Seizure	  
	TERRESTRIAL-BASED	Cyberattacks	  
		Jamming and Spoofing	 
		Direct-Ascent ASAT	  
		Air, Sea, and Land Kinetic Attacks	   



SCENARIOS FOR DEFENSIVE COUNTERSPACE OPERATIONS

The effectiveness of defenses in deterring or defeating attacks in space depends on the context of the situation and the operational concepts used to employ them. To test the space defenses posited and gain further insight into how they could be applied in crisis situations, the study team developed four hypothetical scenarios. The scenarios range from outright aggression in space to the perhaps more likely yet uncertain scenarios with low attribution or reversible effects.

The scenarios were presented to a group of space and national security experts in a series of workshops to understand how policymakers might use space defenses in different situations. The workshops were conducted on a not-for-attribution basis. During the workshops, participants were presented with questions at the end of each scenario or part of a scenario to assess their interpretation of the events posited and possible actions to defend against perceived attacks. Participants were also asked to assess options to es-

calate or deescalate the conflict given the scenario presented.

The workshops were used to refine the description and framework of space defenses in Chapter 3, the concepts for employing defenses in Chapter 4, and the scenarios themselves. The sections below provide a description of the scenarios, the questions asked of the participants, and some of the key findings from the expert discussions that followed each scenario. The scenarios are intentionally opened and designed to provoke discussion about how best to respond and whether certain defensive capabilities would be useful as part of a response. They are set in the near future to allow for some changes in the world, but not so far in the future as to allow great leaps in technology. Scenarios 1 and 3 are divided into two parts, where the second part builds on the information provided in the first part. Otherwise, the four scenarios are assumed to occur independent of one another. While the scenarios are designed to be realistic, the specific events, locations, capabilities,

and nations involved are largely fictional and only intended to represent plausible scenarios in which conflict could begin or extend to space.

SCENARIO 1 RUSSIAN INCURSION INTO THE BALTICS

PART A: ESCALATING TENSIONS

Amid renewed concerns about the North Atlantic Treaty Organization (NATO) moving to create permanent bases for the Enhanced Forward Presence (EFP) forces in the Baltics, Russian president Vladimir Putin decides he must push back against further NATO consolidation. Unlike in the case of Crimea, Putin recognizes that the Baltic states are part of NATO and that all NATO states have a treaty

obligation to defend them. Yet Putin has been clear about what is at stake if his efforts at the “protection of Russian citizens” are actively opposed by the West.



Russian cyber forces have engineered a massive Facebook, Twitter, and Instagram social media push to create an active image of Russian citizens being persecuted and tortured in the southern and eastern Baltics. Russian diplomats warn the Baltic states that these actions must stop, or they will be forced to act. Russian and Belarusian “citizen militias” have begun to move into Baltic towns in southern Lithuania and eastern Latvia. In response, Lithuania has blocked Russian access to Kaliningrad, something that is normally allowed under Facilitated Transit Document (FTD) provisions.

After claiming the Lithuanian blockade is an act of aggression, Russia begins a cyberattack on the Lithuanian terrestrial telecommunications networks, effectively bringing them down. Russia also jams all satellite communications (SATCOM) into the country, including all military and NATO communications other than the protected Advanced Extremely High Frequency (AEHF) SATCOM. The United States and NATO grow more alarmed, and leaders call a formal meeting of the North Atlantic Council.

As these discussions begin, the Russian Federal Communications Agency (Rossvyaz) announces the movement of one of its civilian communications satellites in GEO, *Ekspress AM7*, from its slot at 40°E to a new slot at 53°E, replacing *Ekspress AM6*.⁸⁹ During transit, Rossvyaz announces that it has lost control of the satellite, which is now continuing its eastward drift directly into the path of the United States’ *AEHF 5* satellite at 54°E. Rossvyaz is finally able to stop the satellite’s drift, but by that time it is dangerously close to



Map depicting hypothetical Lithuanian blockade by Russia and adversary citizen militias.

AEHF 5 and in a position where it intermittently physically blocks the *AEHF* crosslink to other satellites. This significantly degrades the ability of *AEHF 5* to perform its missions because of the time it takes for the network ring among satellites to be reestablished each time it is disrupted. The impact to nuclear command and control is not publicly disclosed. U.S. DoD and intelligence analysts conclude this was an intentional act, but the Russians claim they had no control of the satellite.

To respond, U.S. controllers could reposition *AEHF 5* away from the Russian satellite so that the crosslinks to other satellites are no longer blocked, but leaders are concerned that this would affirm for the Russians (and others) that the nuclear command and control network is being disrupted. U.S. leadership is concerned that the Russian action is an implicit warning that the United States has much to lose in space and in other domains if it actively opposes Russia’s moves in the Baltics.

Questions for Participants:

- Is the Russian SATCOM jamming or the positioning of the *AM7* satellite to block *AEHF* crosslinks in this scenario an act of aggression, a use of force, or an armed attack?
- What are your diplomatic and informational options (public and private), and what are the pros and cons of each?
- What are the pros and cons of different responses in space?
 - ◊ Maneuver the *AEHF 5* satellite under the guise of using an “abundance of caution” to protect against a possible in-space collision, though this will break the nuclear command and control link for several additional days.
 - ◊ Coordinate with the *AM7* satellite manufacturer to surreptitiously gain control of the satellite in a collaboration between USSPACECOM and U.S. Cyber Command (USCYBERCOM).



- ◊ Inform Russia that its satellite is now a hazard to navigation and that, if it cannot regain control, the United States will hire a commercial on-orbit servicing vehicle to relocate the satellite to a graveyard orbit.
- ◊ Jam Russian SATCOM across the region, and request support from USCYBERCOM to attack Russian local terrestrial networks.
- ◊ Other options?
- What additional capabilities do you wish you had?
 - ◊ Ability to maneuver while maintaining cross links.
 - ◊ Pre-developed cyber capability for uncooperative commanding of a wide variety of commercial geosynchronous satellites.
 - ◊ On-orbit availability of DoD-owned servicing and seizure satellites.
 - ◊ Satellites with onboard self-defense capabilities (kinetic or non-kinetic).
 - ◊ Internationally acknowledged right to remove hazards to navigation in space.
 - ◊ Other capabilities?

PART B: CONTINUED ESCALATION

The standoff in the Baltics has continued for months while Russia has amassed active-duty troops along the Lithuanian border. Putin warns the United States of dire consequences if it or NATO interferes in the Baltics. A previously undetected Russian space mine maneuvers next to an older decommissioned GPS satellite and detonates, destroying the satellite and generating debris in MEO. Only the United States and Russia can detect what happened, since no other nations or private firms actively monitor

inactive MEO satellites. The United States protests to the United Nations, but Russia claims it must have been an internal propellant tank explosion on the old GPS satellite. The Russians point out that no object was reported near the old GPS satellite in the officially published U.S. satellite catalog. The Russian spacecraft had been recently spotted by the U.S. Space Force, but it had not yet been identified and thus was not catalogued.

USSPACECOM begins an intensive SDA clearing exercise for all GPS satellites and finds what are believed to be Russian space mines located near many other active GPS satellites, meaning they were either previously missed or were positioned in the last several weeks. USSPACECOM cannot be sure how many GPS satellites are threatened because the mines are small and come in and out of view periodically. U.S. leaders want to strongly oppose Russian actions but require assurance from USSPACECOM that the GPS constellation can be kept safe to avoid the potential economic impact of a GPS degradation.

Questions for Participants:

- Is the Russian detonation of a mine and destruction of a decommissioned GPS satellite in this scenario an act of aggression, a use of force, or an armed attack? Would the answer be different if it was an operational GPS satellite?
- What are your diplomatic and informational options (public and private), and what are the pros and cons of each?
- What are the pros and cons of different responses in space?
 - ◊ Begin a coordinated maneuver of all GPS satellites away from the space mines but recognize that

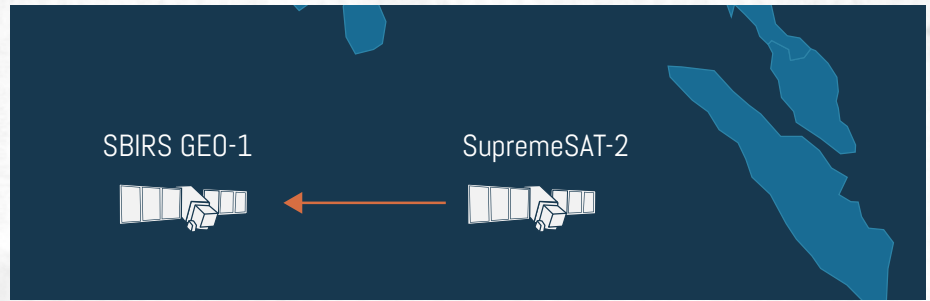
GPS accuracy will be affected for many weeks.

- ◊ Try to jam the communication uplink to the Russian mines.
- ◊ Rapidly purchase and launch a series of active debris removal satellites from a commercial company and use them to remove the space mines.
- ◊ Destroy a Russian GLONASS satellite with a kinetic attack.
- ◊ Issue a demarche to Russia declaring that the loss of any additional GPS satellites will be viewed as an armed attack that will force the United States to respond in other domains.
- ◊ Other options?
- What additional capabilities do you wish you had?
 - ◊ Enhanced SDA observational and analytical capabilities that could have warned of Russian mines positioning in MEO well before they were in place.
 - ◊ Ability to maneuver while maintaining PNT services.
 - ◊ Larger reserves of propellant for additional maneuver capability on the GPS satellites.
 - ◊ More robust GPS receivers that can use other signals to blunt the impact of GPS losses.
 - ◊ A U.S. ground-based navigation system capability as a GPS backup located in the continental United States.
 - ◊ GPS satellites with onboard self-defense capabilities (kinetic or non-kinetic).
 - ◊ More on-orbit spares for GPS (current GPS constellation is ~30 satellites, but only 24 are needed to function properly).
 - ◊ Others?

FINDINGS

This scenario reinforced how essential SDA data is for understanding attacks in the space domain. Experts recommended expanding SDA capabilities by tapping into commercial or international partner capabilities and fielding additional space-based SDA systems. They lamented that the United States' SDA capabilities significantly hampered decisionmaking in this scenario, noting that a better understanding of the space environment would have allowed for more options and better flexibility in decisions. With both space challenges presented in this scenario—the blocking of AEHF satellite crosslinks in GEO and the space mines next to GPS satellites in MEO—participants noted that improved attribution capabilities would have allowed decisionmakers to better assess the intent and credibility of perceived Russian threats.

Participants also emphasized that clearer norms and processes for deal-



SupremeSAT-2 moving toward SBIRS GEO-1 over the Laccadive Sea just south of Sri Lanka in scenario.

ing with hazards in space would have helped facilitate a better understanding of Russian actions. Some participants commented that communicating in advance clear thresholds for escalation and a range of defensive actions that would be triggered could have prevented certain actions, such as the space mine attack. Experts assessed that the starting point should be to establish international norms and rules of the road for acceptable behavior in space. Established norms could act as tripwires that, if crossed, would signal malicious intent.



often cause interference with nearby satellites as they drift by.

The Chinese blame the failures, without evidence, on a U.S. cyber intrusion in its industrial base.

In early April, China is set to begin its annual strategic forces exercise that includes the launch of multiple missiles and other strategic military systems over the course of a three-week period. Just before the exercise starts, Sri Lanka announces it has lost control of *SupremeSat-2*, which is from the same Chinese manufacturers as the two other failed satellites.

SupremeSAT-2 is rapidly drifting to the west out of control. The U.S. Combined Space Operations Center (CSpOC) calculates that it will pass close to *SBIRS GEO-1*, a U.S. military missile warning satellite, although the likelihood of collision is very low. However, the high-powered Ka band payload on-board *SupremeSat-2* will begin to interfere with the *SBIRS* communications payload as it drifts closer. The likely consequence is that *SBIRS GEO-1* will be unable to conduct its mission reliably for up to a week as *SupremeSAT-2* passes. This week happens to fall near the peak of the planned Chinese military exercise in the region covered by *SBIRS GEO-1*. The annual Chinese strategic forces exercise involves the launch of multiple missiles and other strategic military systems the *SBIRS* satellite would normally observe.

SCENARIO 2

POSSIBLE HIJACKED SATELLITE

The United States and its allies are increasingly concerned that more nations, especially those in Asia, are turning to China as their supplier of choice for space systems. In many cases, the Chinese have provided a complete turn-key system along with financing that is extremely attractive to less affluent nations. As a result, some 10 percent of all GEO satellites in operation are now Chinese made. In line with these trends, Sri Lanka recently replaced its first satellite, *SupremeSAT-1*, with the Chinese-built *SupremeSAT-2*, a very high-powered C, Ku, and Ka- band communication satellite located at 87.5°E longitude.

In the last six months, two different Chinese-built satellites experienced uncontrolled commanding events. Despite their best efforts, the satellite operators have not been able to regain control of these satellites. Both were communication satellites launched in the last five years, and both are now drifting relatively harmlessly around the GEO belt. The communications payloads on the satellites are active and

USSTRATCOM requests support from USSPACECOM to help mitigate the critical loss of missile warning and technical intelligence capabilities during the Chinese exercise. These capabilities are needed to monitor Chinese activities to ensure it is not threatening one of its neighbors and provide valuable intelligence on Chinese military capabilities.

Questions for Participants:

- Is the movement and interference caused by *SupremeSAT-2* in this scenario an act of aggression, a use of force, or an armed attack?
- What are your diplomatic and informational options (public and private), and what are the pros and cons of each?
- What are some response options along with their pros and cons?
 - ◊ Maneuver the SBIRS satellite into an eastward drift to minimize the overlap time between the two systems and limit the outage.
 - ◊ Request that the Chinese assist Sri Lanka in regaining control of its satellite.
 - ◊ Maneuver two other SBIRS satellites into new positions to “pinch” the hole between them to recover coverage of most of the area that will be affected.
 - ◊ Do nothing so as not to admit that the interference has harmed missile warning capabilities.
 - ◊ Other options?
- What additional capabilities do you wish you had?
 - ◊ Laser crosslinks or other backup communications channels for missile warning capabilities to provide diverse communications options.
 - ◊ More distributed and proliferated missile warning capabilities such as commercially hosted payloads and

MEO or LEO overlays.

- ◊ Additional on-orbit spares for missile warning.
- ◊ Satellites with onboard self-defense capabilities (kinetic or non-kinetic).
- ◊ Pre-developed cyber capability for uncooperative commanding of a wide variety of commercial geosynchronous satellites.
- ◊ Satellites that have onboard capabilities to more easily attribute and respond to hostile acts.
- ◊ Others?

FINDINGS

Like Scenario 1, many participants wanted better information about the satellite anomaly through exquisite SDA. Specifically, participants wanted more on-orbit SDA capabilities so that an inspector satellite could maneuver nearby and take a closer look to verify Chinese and Sri Lankan statements on the condition of the satellite. Also like Scenario 1, participants noted the advantage of having pre-established norms of behavior that

could have made communication easier between the involved nations and the United Nations.

The potential effects this scenario posed on such a critical U.S. national security system caused great concern. Participants called for more SBIRS satellites on-orbit as backups and better crosslinks between satellites so that the one affected could be taken offline until the situation resolved itself. Participants also noted that if the United States had a proliferated LEO constellation for missile warning, the loss of one satellite would matter much less and the mission could continue somewhat unaffected.

The workshop participants also remarked that an on-orbit servicing satellite would have been greatly helpful in this scenario. If the United States had an on-orbit servicing capability in GEO at the time, it could have offered Sri Lanka assistance in maneuvering its satellite to a less-disruptive orbit until the problem could be addressed.

SCENARIO 3

ESCALATING TENSIONS IN THE SOUTH CHINA SEA

PART A: ECONOMIC COERCION

Just years after China declared its BeiDou navigation system fully operational, BeiDou has now been adopted by dozens of neighboring Asian nations as their preferred navigation system, due in no small part to Chinese Belt and Road Initiative incentives. After years of high-profile U.S. sanctions on Chinese technology companies and the repeated refusal of the U.S. Federal Communications Commission (FCC) to approve BeiDou use in the United States, the Chinese have reached a breaking point.

China declares that GPS navigation products are tools of the U.S. military and can no longer be used within Chinese territory, including its disputed maritime and air space

claims in the South China Sea. China convinces many of its Belt and Road clients to follow suit and restrict the use of GPS in their territory as well. Furthermore, China states that this mandate will be enforced by selective intermittent jamming of U.S. GPS frequencies and signals “at the times and places of our choosing.” International air and maritime carriers not currently using BeiDou are given six months to transition.

China and its client states in the region begin to locate GPS jammers around their borders and on natural and artificial islands in the South China Sea. The Chinese jammers are burst mode jammers, which routinely emit bursts of noise into both the L1 and L2 bands to prevent GPS receivers from maintaining a continuous lock on the signals within a large zone.

The countries involved and their distributed island geography effectively create a no-GPS-usage zone for anyone using the GPS civilian signal (C/A Code) within broad parts of the South China Sea. Traditional P(Y) code and Selective Availability Anti-spoofing Module (SAASM) receivers are also impacted for military users who have not upgraded to M-code receivers.⁹⁰

The United States and its allies protest the Chinese action to the International Telecommunication Union (ITU), but the ITU notes that the question of landing rights for GPS signals has never been taken up or requested by the United States. Therefore, the GPS signal is not protected, and sovereign nations can refuse to allow the GPS signals to be received and used within their territory, just as the United States has barred non-GPS GNSS signals from being used in its territory.⁹¹ The ITU does not address the issue of Chinese sovereignty over disputed islands in the South China Sea.

The first Chinese jamming campaign occurs on the eve of the biennial Rim of the

Pacific (RIMPAC) exercise among U.S. and partner nations in the region, and both civilian and military air and maritime users begin to feel the impacts immediately. The U.S. Intelligence Community, using government and commercial assets, begins to map the locations of the jammers. Several images of jamming locations appear in published think tank reports that expose what the Chinese are doing. Fearing that the United States may try to target the jammers under the cover of the ongoing exercise, the Chinese announce that any U.S. satellites collecting intelligence over Chinese territory will face possible engagement by mobile ground-based lasers “intended to prevent illegal spying.” As Chinese satellite blinding activities begin, several U.S. commercial imagery satellite operators report permanent damage to their systems. Some U.S. classified satellite imagery systems temporarily cease operation in the region for fear of damage.

Questions for Participants:

- Are the GPS jamming and laser blinding attacks in this scenario acts of aggression, uses of force, or armed attacks?
- What are your diplomatic and informational options (public and private), and what are the pros and cons of each?
- What are the pros and cons of different responses in space?
 - ◊ Jam all satellite communications between Chinese island outposts and the mainland and enlist the Navy to sever undersea cables to the islands as well.
 - ◊ Use maximum flex power capabilities within the GPS system to boost C/A and P(Y) signals by robbing power from the M-code signal, recognizing that there will be an impact to those who have upgraded to M-code receivers.

- ◊ Begin emergency deployment of M-Code receivers to the most critical U.S. and allied ships, whether commercial or military, to restore freedom of navigation in the area.
- ◊ Direct the National Reconnaissance Office (NRO) and National Geospatial-Intelligence Agency (NGA) to prioritize radar imaging in the Indo-PACOM region and develop a means to responsively locate mobile lasers to alert commercial and government satellite imagers where they should not point.
- ◊ Blind Chinese imagery satellites over U.S. territory.
- ◊ Jam BeiDou signals in the South China Sea.
- ◊ Other options?
- What additional capabilities do you wish you had?
 - ◊ Multi-GNSS receivers to allow U.S. forces to use BeiDou and other systems when GPS is not available.
 - ◊ Greater fielding of anti-jam antennae on U.S. platforms.
 - ◊ Capability for greater anti-jam power in the GPS system.
 - ◊ Ability to field long-endurance, high-altitude aircraft or blimps to provide backup signals in affected regions.
 - ◊ Laser protection technologies that could be shared with U.S. commercial imagery providers and mandated as a condition of U.S. government imagery contracts.
 - ◊ Ability to transparently task allied satellite imagery systems as easily as U.S. government and commercial assets.
 - ◊ Ability to rapidly reconstitute imagery satellites if they are blinded.
 - ◊ Others?



PART B: ESCALATING TENSIONS ON THE ROAD TO ARMED CONFLICT

The United States responds to the Chinese actions in multiple domains, including sanctions on shipping, SATCOM jamming, and cyberattacks on Chinese outposts in the South China Sea. The Chinese respond by similarly jamming U.S. SATCOM capabilities, both commercial and military, from the mainland. The U.S. military's Mobile User Objective System (MUOS) ultra-high frequency service is down, as is the commercial Ku band, normally used to support drone operations. Jamming of the Wideband Global SATCOM (WGS) system severely limits its capacity. U.S. and allied naval forces in the South China Sea that do not have AEHF radios installed are now without reliable or robust communication services, severely constraining their operations. U.S. commercial shipping is essentially sailing blind without communication or GPS, which causes trade in the region to grind to a halt.

The United States begins to maneuver two WGS satellites into better positions to restore some SATCOM capacity in the region and works with the CSpOC to quietly arrange alternative communication systems using non-U.S. commercial or allied military satellites. The United States also initiates a campaign of Geosynchronous Space Situational Awareness Program (GSSAP) close inspections on Chinese GEO assets to signal U.S. resolve. The Chinese begin to intercept and board U.S. commercial ships, which the Chinese assert have sailed into Chinese-claimed waters and are violating its prohibition on the use of GPS.

As tensions further escalate, U.S. space surveillance systems detect several

previously unknown objects that seem to have originated from the Earth-Moon L2 Lagrange point (where a Chinese lunar relay satellite had been positioned since 2018) now accelerating toward the Earth. The final trajectory and timing are uncertain, but it is clear they will cross the GEO belt within two days. The National Space Defense Center calculates that many GEO objects could be at risk, but it cannot yet tell which ones.

Questions for Participants:

- Was the U.S. response posited at the beginning of Part B proportional to the actions that occurred in Part A, and was it allowable under the Law of Armed Conflict?
- Are the Chinese SATCOM jamming and the movement of its lunar assets in this scenario acts of aggression, uses of force, or armed attacks?
- What are your diplomatic and informational options (public and private), and what are the pros and cons of each?
- What are the pros and cons of different responses in space?
 - ◊ Free up bandwidth on AEHF for more tactical use by naval forces (at the expense of strategic AEHF users).
 - ◊ Provide guarantees to U.S. and allied commercial SATCOM providers that they will be reimbursed for loss of satellite lifetime and revenues if they can more quickly reposition their satellites and free up bandwidth for use in the area.
 - ◊ Request support from USCYBERCOM to disable both mainland Chinese jammers and space surveillance sites to prevent accurate tracking of U.S. GEO satellites.
 - ◊ Prepare maneuver plans for all

U.S. GEO satellites for rapid execution once possible crossing points for the reentering lunar satellites are determined.

- ◊ Identify and jam the communication links to the reentering Chinese lunar satellites.
- What additional capabilities do you wish you had?
 - ◊ Greater access to tactically protected AEHF satellite communications for all U.S. forces.
 - ◊ Extensive LEO communication capabilities which cannot be easily jammed over the horizon, especially for small tactical users constrained to MUOS.
 - ◊ Proliferated constellations in diversified orbits to complicate Chinese jamming and other forms of attack.
 - ◊ More extensive deep space surveillance to track and catalog objects beyond GEO.
 - ◊ Existing Civil Reserve Air Fleet (CRAF)-like arrangements with U.S. commercial SATCOM providers to rapidly shore up communication capabilities in a crisis.
 - ◊ Others?

FINDINGS

While participants did not consider GPS jamming alone an act of war, many considered it a clear use of force and a potential act of aggression as it was used in the scenario. Some noted that jamming and spoofing are two of the most frequently used counter-space weapons and that, to protect against it, the United States should accelerate the fielding of M-code GPS receivers to make them harder to jam. Experts also noted that multi-GNSS receivers, or the ability to use other PNT signals from constellations such as Galileo, BeiDou, and GLONASS, would have been useful in this situa-

tion because it would have made China's GPS jamming ineffective.

Some participants considered using active defensive operations in this scenario, including jamming of BeiDou within the region. Several felt that escalating to widespread BeiDou jamming operations beyond the region could be sufficient to deter further Chinese action. However, a global BeiDou jamming operation would require support from allies and partners as well as a robust PNT jamming capability. Other proportional responses suggested by participants included dazzling or

blinding Chinese imagery satellites, using the Navy to forcibly restore freedom of navigation in the South China Sea, and retaliating with economic sanctions against China for the disruption of commercial shipping.

Participants emphasized the need for reconstitution capabilities to replace lost or degraded ISR capabilities quickly, including more imagery satellites, pseudo-satellites, or other high-altitude ISR systems. They also noted the need for more extensive deep space surveillance to track and catalog objects beyond GEO.

sian sword), are responsible for space-based jamming of the broadcasts.

Months later, the two Shamshir satellites undergo a high-impulse maneuver, putting them into a westward drift in GEO toward the United States. The jamming of Radio Farda ceases, but U.S. intelligence does not see an immediate threat to any DoD or IC assets because it judges that these satellites are limited to civilian SATCOM frequencies.

U.S. military and commercial sensors later determine that the two Shamshir satellites are nearing the orbital slot currently occupied by three U.S. DirecTV satellites located at 99.2°W longitude.⁹² As the two Shamshir satellites come within close proximity to the first DirecTV satellite, it begins to experience significant interference. Over the course of the next few days, DirecTV loses all contact with the satellite. Telemetry streams indicate that the front-end low noise amplifier on the receiver side was highly saturated (overloaded) as one of the Shamshir satellites approached, and it eventually burned out the amplifier.

Within a week, all three DirecTV satellites in this orbital slot are non-operational. DirecTV maintains robust on-orbit spares, with a second set of 3 satellites at 102.8°W, but the loss of their fleet at 99.2°W significantly impacts DirecTV customers. As the Shamshir satellites begin a second drift toward the 102.8°W orbital slot, Iran informs the United States that it will continue to attack U.S. commercial broadcast satellites unless the U.S. sanctions are lifted. The Super Bowl is next week, and the loss of these last three satellites will impact millions of North American customers.

Current intelligence indicates that the satellites are being controlled from a high-powered base station in Venezuela. The United States judges that it could likely jam the uplink, but this would re-

SCENARIO 4

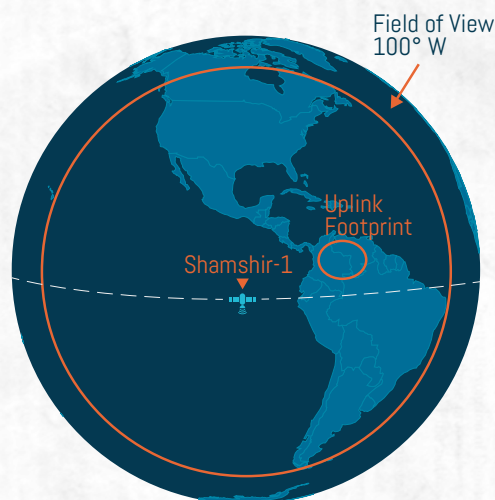
COMMERCIAL SPACE SYSTEM PROTECTION

Hostilities between the United States and Iran have once again been flaring up over Iran's nuclear program. New, more onerous sanctions are taking their toll on the Iranian economy, and Iran has promised strong retaliation. Iran is now a player in the space domain as well, and it succeeds in launching two small satellites into GEO with the help of Russia and China. Iran claims these satellites are for experimental purposes. A close inspection by U.S. GSSAP inspector

satellites reveals two large, highly directional antenna dishes on the satellites, which seem more consistent with a co-orbital jamming capability.



In recent months U.S. broadcasts of Radio Farda, the Iranian branch of Radio Free Europe, has suffered country-wide outages in Iran. USSPACECOM and the U.S. Intelligence Community suspect that the Iranian satellites, nicknamed "Shamshir" (after a type of Per-



CLICK TO
FLY BACK TO
THE CONTENTS

quire jammers positioned very close to Venezuela. Aruba, part of the Kingdom of the Netherlands, is the most likely potential basing option. The United States refuses to comply with Iran's demands to lift the sanctions and instead directs the military to develop options to stop the Iranian satellites from carrying out further attacks.

Questions for Participants:

- Is the interference and damage caused by the Shamshir satellites in this scenario a hostile act, an act of aggression, a use of force, or an armed attack?
- What are your diplomatic and informational options (public and private), and what are the pros and cons of each?
- What are some response options along with their pros and cons?
 - ◊ Request the Kingdom of the Netherlands to allow the United States to position a jammer on the island of Aruba to jam the Shamshir uplink but recognize that it might take weeks to receive permission.
 - ◊ Base a jammer on a U.S. Navy ship in international waters off the coast of Venezuela to jam Iranian uplinks to its satellites.
 - ◊ Request assistance from USCYBERCOM to disable the ground station in Venezuela.
 - ◊ Request assistance from USSOCOM to deploy a team to physically sabotage the ground station in Venezuela.
 - ◊ Assist DirectTV in tracking the Shamshir satellites, and provide maneuver and antenna pointing options that would prevent damage but would also take the DirecTV satellites out of service while the actions are underway.
 - ◊ Other options?

- What additional capabilities do you wish you had?
 - ◊ More practical exercises and training with civilian and commercial satellite operators to understand how to react more quickly in these types of scenarios.
 - ◊ Airborne or shipborne jamming systems to allow more responsive uplink jamming options.
 - ◊ On-orbit defensive satellites in supersynchronous orbit to rapidly reach any longitude in GEO.
 - ◊ Ground-based or co-orbital ASAT weapons capable of disabling satellites in GEO using HPM weapons.
 - ◊ Others?

FINDINGS

Since this aggressive action against a commercial company in space was relatively unprecedented, participants discussed proportionality and how deeply the U.S. military should be involved in such a situation. Economic sanctions and other non-space responses were considered first, before moving to actions affecting the space domain. Again, it was emphasized by experts that if established norms of behavior were in place, these actions may have been deterred or Iran would have more international pressure to rectify its actions.

KEY TAKEAWAYS

Throughout the workshops, several different operational concepts were considered and discussed among experts on how best to protect U.S. assets from counterspace attacks. It was widely agreed that no single defensive concept would be sufficient to protect against all counterspace attacks. Therefore, the U.S. government needs multiple concepts of operation and defensive capabilities to provide a wide range of options to decisionmakers in a crisis.

A common thread throughout all the scenarios was the need for better SDA. Accurate, timely, and comprehensive SDA is fundamental to providing decisionmakers with the information they need to properly assess options. While ground-based SDA is integral, many experts suggested further investments in space-based SDA systems. These space-based systems could include on-orbit radars and inspector satellites that can maneuver to provide more information during a crisis. It was also clear that without SDA for cislunar and lunar space, U.S. decisionmakers would be at a great disadvantage if adversary space operations extended beyond the typical Earth orbits.

Norms, rules of the road, and well-communicated thresholds also emerged in the discussions for each scenario. Participants agreed that without widely accepted norms of behavior in space, the United States is in murky waters. While norms will likely be disregarded once a conflict begins, they are useful in providing indications and warnings and shaping the environment prior to conflict. Participants also noted that norms in other domains, such as approaching the perimeter of a military base or a speedboat approaching a warship at sea, often do not translate well into the space domain. For example, it is widely understood that using deadly force to stop someone from breaching or attempting to breach the perimeter of a military base is an appropriate and justifiable use of military force. But it is not widely accepted that similar capabilities in space, such as a kinetic shoot-back system, can be used to stop another nation's satellite from closely approaching a military satellite. While close approaches occur in the air domain, such as aircraft from one nation flying dangerously close to U.S. aircraft operating in international airspace, a key difference is that in the air domain



both sides eventually must go back to their respective bases. In space, a close approach—including one that interferes with a satellite’s mission capabilities—can be maintained continuously for months or years.

In space, all objects are constantly in motion, and therefore linear rules of engagement, such as maintaining safety perimeters around critical assets, are not practical. A simple keep-out distance around satellites is not sufficient because the threat another space object poses depends on more than just distance. Defenders must be concerned about the change in velocity (delta V) needed for one satellite to intersect another, the ability of other satellites to maneuver, recent maneuvers, and the capabilities of an approaching satellite. Moreover, all of this is complicated by imperfect, delayed, and intermittent information on what is happening in the space domain.

It was commonly agreed in the workshops that a proportional response to an attack in space may not be an action in the space domain. This may cause or aggravate tensions between USSPACECOM, USSTRATCOM, and other regional combatant commands, depending on which countries are involved in the conflict. A key takeaway from the workshops was that it is important to use such scenarios within DoD and among allies to practice and determine how the chain of command and responsibilities for being the supported and supporting command might shift during a conflict.

Experts also agreed that more information on or better options for cyberattacks on and against space systems is essential. Cyberattacks were often viewed as a possible convenient and proportional response, especially if the cyberattacks could be directed against the perpetrating adversary space sys-

tems. Investing in cyber capabilities and the flexibility of such counterspace attacks or defensive options would allow decisionmakers to have more attractive defensive options.



CONCLUSIONS AND RECOMMENDATIONS

The United States maintains a distinct strategic advantage in space. While China and Russia have significant space capabilities of their own, the main security challenge they pose in space is the wide array of counterspace weapons they continue to develop, test, and proliferate. Russia and China are arguably making advances in counterspace weapons faster than the United States is improving its defenses against these threats. While the public discourse about the threats to space systems—not just from Russia and China but also from lesser powers such as North Korea and Iran—has become more prominent in recent years, the lack of a concurrent discussion about how to defend space systems against these threats has left some to incorrectly conclude that space is not defensible.

Given the myriad of defensive options available, the question facing policymakers is not whether space is defensible but rather which defenses the military should be investing in and how they should be employed. This conversation is especially important now because the U.S. military is in the process

“Numbing the pain for a while will make it worse when you finally feel it.”

ALBUS DUMBLEDORE, HARRY POTTER AND THE GOBLET OF FIRE

of modernizing many of its key satellite constellations. The decisions made over the coming months and years about what types of space architectures to field and which defenses to incorporate will have repercussions for the life of these systems. As this report demonstrates, a wide range of active and passive defenses are available to protect space systems and the ground infrastructure they depend upon from different types of threats.

Space defenses can be organized into three categories of passive defenses (architectural, technical, and operational) and two categories of active defenses (space-based and terrestrial-based). Among the architectural passive defenses explored in this study, one of the key takeaways is that distributed, diversified, and proliferated constellations can all be used in various combinations to complicate the targeting calculus of an adversary and reduce the benefits of attacking any single satellite. Disaggregating space missions to separate platforms may reduce the risks of miscalculation and inadvertent escalation in a conflict, but an adversary may not be able to distinguish

between satellites intended for different missions or may not trust this distinction. Disaggregation of strategic and tactical missions may also make attacking a tactical system more attractive because it reduces the risk of strategic escalation.

Technical types of passive defenses, such as electromagnetic shielding, jam-resistant waveforms, and antenna nulling, can make systems more difficult to attack and can limit the degradation in capabilities that occurs during an attack. The main downside for technical defenses is that they can add cost, weight, and complexity to systems. Space domain awareness, particularly from space-based systems, stands out as particularly important because it is helpful across a wide variety of scenarios and is a key enabler that makes many other types of space defenses more effective. The need to improve space domain awareness capabilities was a consistent theme throughout the workshops conducted as part of this study.

Operational passive defenses, such as satellite maneuver, stealth, deception, and decoys, can be used to make satellites difficult to find, track, and target. Rapid deployment can be used to

launch new capabilities an adversary may not be expecting once a conflict begins, and reconstitution can be used to replace systems that are damaged or destroyed. However, maneuver is not likely to be a successful defense on its own because ASAT warheads have an inherent maneuver advantage over large satellites, and reconstitution capabilities may not be useful in a conflict until an adversary's counterspace capabilities are neutralized.

Space-based active defenses protect space systems by disrupting or destroying an adversary's counterspace weapons, effectively raising the costs of attacking space systems. Non-kinetic active defenses can be deployed in space to jam or spoof adversary radars systems, to blind optical or infrared sensors, or to create physically damaging effects on ASAT weapons using directed energy systems. A kinetic shoot-back system can use projectiles, guided warheads, or small satellites to physically impact a threat in space. These kinetic and non-kinetic systems can be deployed on the satellites they protect or on separate guardian satellites that orbit nearby or roam among satellites, creating a zone defense. The workshops and scenarios highlighted the value of having a satellite that can physically seize objects in space to move or disable them. This could be particularly useful in situations where there is ambiguity about a threatening object's real status and capabilities or where decisionmakers may want to mitigate the risk of orbital debris.

Terrestrial-based active defenses can be used to target counterspace weapons in space and the ground systems that control and operate these weapons. Cyberattacks and jamming or spoofing of command uplinks to counterspace weapons proved to be attractive options in the workshop scenarios, although participants noted the uncer-

tainty about whether such attacks would be feasible and effective in a crisis. Terrestrial-based kinetic forms of attack to disable an adversary's counterspace weapons, such as a direct-ascent ASAT attack in space or firing cruise missiles at counterspace ground sites, tended to be viewed as more escalatory options that would likely be reserved until armed conflict was already underway on the ground. The United States and its allies and partners have a strong incentive to avoid using kinetic attacks in space that are likely to produce orbital debris, even if such defenses may be warranted.

The workshops and hypothetical scenarios for conflict in space also highlighted many ambiguities that exist in space. As a physically distant and inhospitable environment, it can be difficult to monitor and understand adversary capabilities and intentions in the space domain, similar to the difficulties encountered in undersea operations. Dual-use space systems that can be used for both peaceful and military purposes and the lack of widely accepted norms of behavior in space further compound this problem of understanding actions and intents. These factors combine to make it difficult to determine proportionality of a response, including whether certain defensive actions are warranted. Thresholds for triggering defensive actions or offensive escalation may appear fluid or confusing to an opponent because these thresholds can be non-linear and highly context dependent. This study also found that there is significant overlap between the capabilities needed for defensive and offensive counterspace operations, particularly for active forms of space defense. For example, an adversary could view a space-based shoot-back system, whether kinetic or non-kinetic, as no different than an offensive space-based ASAT system or a space-based missile interceptor system.

A broad conclusion from this study is that the character of space warfare is evolving. This evolution is being driven by how the major military powers view and use the space domain—particularly whether it is primarily an information domain or a physical domain. The information domain school of thought emphasizes the use of space for remote sensing and communications. It is an enabler for forces in the other domains and a key component of battle networks and the sensor-to-shooter kill chain. This school of thought has dominated the planning for conflict that could begin or extend into space for nearly six decades.

In contrast, the physical domain school of thought places relatively more emphasis on the physical components of operations in space, including space launch, the application of force in space or from space, and the use of space for transportation, logistics, and other physical support functions. While some of these more physically focused military space missions are still in their infancy, they are likely to become increasingly prominent in the coming years due to reductions in the cost of launch and the proliferation of counterspace weapons and space defenses.

The challenge for space strategists is to anticipate how this gradual shift from space being more focused on information operations to physical operations will proceed. The evolution in the character of space conflict and how quickly that evolution proceeds directly impacts the types of space defenses and operational concepts the military should be developing today. With the evolving character of space warfare in mind, this study recommends the following priorities, actions, and additional analysis.

"You sort of start thinking anything's possible if you've got enough nerve."

GINNY WEASLEY,
HARRY POTTER
AND THE
HALF-BLOOD
PRINCE

These recommendations are made without regard for what may already exist or be in development.

- A priority should be placed on investments in improved space domain awareness capabilities, to include more space-based sensors, better integration with commercial and friendly foreign government systems, and the use of artificial intelligence to analyze data and form a better understanding of capabilities and intentions.
- Additional effort should be placed on developing improved indications and warnings for space that give decisionmakers more time and information to tailor potential defensive responses to the specific circumstances of a conflict.
- New space architectures are needed that use a combination of distribution, proliferation, and diversification of orbits. These new architectures do not necessarily need to replace legacy architectures but rather can be used to supplement and diversify capabilities that already exist.
- Non-kinetic active defenses, such as onboard jamming and lasing systems, are needed to thwart kinetic attacks against high-value satellites. A physical seizure capability should also be explored that could double as an inspector and on-orbit servicing satellite.
- New options should be considered to improve DoD's integration with commercial space operators and better leverage existing space systems for national security purposes. For example, DoD could create a program like the Civil Reserve Air Fleet (CRAF) with commercial space operators and use that program to incentivize investments in better passive defenses for commercial space systems.

- A better understanding is needed of the operational, political, and strategic risks involved in the use of stealth, maneuver, rapid deployment, and reconstitution before committing significant resources to these passive defenses.

- Further analysis and gaming are needed to explore gray zone competition in space and when it is advantageous (or not) to do nothing in response to an attack or threat of attack.


If space is to remain a source of economic and strategic advantage, the United States must prioritize and expedite its efforts to improve space defenses. Robust space defenses make conflict in space less likely. Many of the architectures and technologies already exist to make space systems more defendable and resilient. Senior leaders in DoD and Congress need to make top-level decisions about which types of defenses to pursue and then provide sustained investments to fund these capabilities to fruition.

"We must choose between what is easy and what is right."

ALBUS DUMBLEDORE, HARRY POTTER AND THE GOBLET OF FIRE




ABOUT THE AUTHORS

 **Todd Harrison** is the director of Defense Budget Analysis and director of the Aerospace Security Project at CSIS. As a senior fellow in the International Security Program, he leads the Center's efforts to provide in-depth, nonpartisan research and analysis of defense funding, space security, and air power issues. He has authored publications on trends in the defense budget, military space systems, threats to space systems, civil space exploration, defense acquisitions, military compensation and readiness, and military force structure, among other topics. He teaches classes on military space systems and the defense budget at the Johns Hopkins School of Advanced International Studies.

Mr. Harrison joined CSIS from the Center for Strategic and Budgetary Assessments, where he was a senior fellow for defense budget studies. He previously worked at Booz Allen Hamilton, where he consulted for the U.S. Air Force on satellite communications systems and supported a variety of other clients evaluating the performance of acquisition programs. Prior to Booz Allen, he worked for AeroAstro Inc. developing advanced space technologies and as a management consultant at Diamond Cluster International. Mr. Harrison served as a captain in the U.S. Air Force Reserves. He is a graduate of the Massachusetts Institute of Technology with both a BS and an MS in aeronautics and astronautics. Mr. Harrison is a proud member of Gryffindor House.

 **Kaitlyn Johnson** is deputy director and fellow of the Aerospace Security Project at the Center for Strategic and International Studies. Ms. Johnson manages the team's strategic planning and research agenda. Her research specializes in topics such as space security, military space systems, commercial space policy, and U.S. air dominance. Previously, Ms. Johnson has written on national security space reorganization, threats against space assets, the commercialization of space, escalation and deterrence dynamics, and defense acquisition trends. Ms. Johnson holds an MA from American University in U.S. foreign policy and national security studies, with a concentration in defense and space security, and a BS from the Georgia Institute of Technology in international affairs. Ms. Johnson is a proud member of Slytherin House.

 **Makena Young** is a research associate with the Aerospace Security Project at the Center for Strategic and International Studies (CSIS). Her research interests include international collaboration, space security, and orbital debris. Prior to joining CSIS, Ms. Young worked for the Federal Aviation Administration as an aerospace engineer, focusing on automatic dependent surveillance-broadcast certification and integration in small aircraft. She holds a BS in aeronautical and astronautical engineering from Purdue University with minors in international relations and environmental engineering. Ms. Young is a proud member of Hufflepuff house.

"Mischief Managed"

HARRY POTTER, HARRY POTTER AND
THE PRISONER OF AZKABAN



ENDNOTES

- 1 Traditional U.S. strategy notionally demarks six phases of operational action: Phase 0 – Shape, Phase I – Deter, Phase II – Seize the Initiative, Phase III – Dominate, Phase IV – Stabilize, and Phase V – Enable Civil Authority.
- 2 Robert Bowman, *Star Wars: A Defense Insider's Case Against the Strategic Defense Initiative* (Los Angeles, CA: Teachers Publications, 1986), 14.
- 3 Laura Grego, “A History of Anti-Satellite Programs,” Union of Concerned Scientists, January 2012, 3, https://www.ucsusa.org/sites/default/files/2019-09/a-history-of-ASAT-programs_lo-res.pdf.
- 4 See Caroline Dorminey and Eric Gomez, eds., *America's Nuclear Crossroads* (Washington, DC: Cato Institute, 2019), 30, <https://www.cato.org/sites/cato.org/files/pdfs/americas-nuclear-crossroads-full.pdf>.
- 5 “Advance Policy Questions for General John W. ‘Jay’ Raymond,” Senate Committee on Armed Services, 116th Cong., 1st sess., 2019, 6, https://www.armed-services.senate.gov/imo/media/doc/Raymond_APQs_06-04-19.pdf.
- 6 “2020 year in review,” Bryce Space and Technologies, October 31, 2020, https://brycetechnology.com/reports/report-documents/Bryce_2020_Year_In_Review.png.
- 7 Starlink passed the 1,000 satellites launched mark in early 2021, China had 363 satellites operational as of March 2020. See: Jeff Foust, “SpaceX surpasses 1,000-satellite mark in latest Starlink launch,” SpaceNews, January 20, 2021, <https://spacenews.com/spacex-surpasses-1000-satellite-mark-in-latest-starlink-launch/>; and China Power Team, “How is China Advancing its Space Launch Capabilities?” China Power, November 5, 2019, Updated August 25, 2020, Accessed January 25, 2021, <https://chinapower.csis.org/china-space-launch/>.
- 8 See: Todd Harrison et al., *Space Threat Assessment 2020* (Washington, DC: CSIS, March 2020), https://aerospace.csis.org/wp-content/uploads/2020/03/Harrison_SpaceThreat-Assessment20_WEB_FINAL-min.pdf; Victoria Samson and Brian Weeden, *Global Counterspace Capabilities* (Washington, DC: Secure World Foundation, April 2020), https://swfound.org/media/206970/swf_counterspace2020_electronic_final.pdf; and U.S. Defense Intelligence Agency, *Challenges to Security in Space* (Washington, D.C., February 2019), https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.
- 9 Joan Johnson-Freese, *Space as a Strategic Asset* (New York: Columbia University Press, 2007), 106.
- 10 Todd Harrison, *International Perspectives on Space Weapons* (Washington, DC: CSIS, May 27, 2020), <https://www.csis.org/analysis/international-perspectives-space-weapons>.
- 11 U.S. Joint Chiefs of Staff, Joint Publication 3-14: Space Operations (Washington, DC: April 2018), I-2, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14ch1.pdf?ver=qmkgYPyKBvslZyrnsWSMCg%3d%3d.
- 12 Harrison, *International Perspectives on Space Weapons*.
- 13 “USSF Mission,” U.S. Space Force, n.d., <https://www.spaceforce.mil/About-Us/About-Space-Force/Mission/>.
- 14 “Mission,” U.S. Space Command, n.d., <https://www.spacecom.mil/Mission/>.
- 15 Kevin L. Pollpeter, Michael S. Chase, and Eric Heginbotham, *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations* (Santa Monica, CA: RAND, 2017), 16, https://www.rand.org/pubs/research_reports/RR2058.html.
- 16 Ibid., 14.
- 17 Harrison et al., *Space Threat Assessment 2020*, 11.
- 18 Ibid., 25.
- 19 There is not one perfect source for determining where Russian counterspace

weapons are housed. Recent suspiciously maneuvering LEO satellites were launched and operated by the Russian Aerospace Forces. However, the the Peresvet ground-based laser, which would ostensibly be operated by the Aerospace Forces, has been tracked to Strategic Missile Forces bases. See: “Russia Launches Kosmos 2542 Military Satellite Abroad Soyuz-2 Rocket,” Defpost, November 27, 2019, <https://defpost.com/russia-launches-kosmos-2542-military-satellite-abroad-soyuz-2-rock-et/>; and Bart Hendrix, “Peresvet: a Russian mobile laser system to dazzle enemy satellites,” The Space Review, June 15, 2020, <https://www.thespacereview.com/article/3967/1>.

- 20 “Defense Space Strategy Summary,” French Ministry of Defense, July 2019, <https://www.defense.gouv.fr/content/download/563617/9727377/synthe%CC%80se%20strate%CC%81gie%20spatiale%20de%20de%CC%81fense.pdf>.
- 21 Harrison et al., *Space Threat Assessment*, 51.
- 22 Vivek Raghuvanshi, “India to launch a defense-based space research agency,” Defense News, June 12, 2019, <https://www.defensenews.com/space/2019/06/12/india-to-launch-a-defense-based-space-research-agency/>.
- 23 Paul Scharre, “The US Military Should Not Be Doubling Down on Space,” Defense One, August 1, 2018, <https://www.defenseone.com/ideas/2018/08/us-military-should-not-be-doubling-down-space/150194/?oref=d-river>.
- 24 Harrison et al., *Space Threat Assessment*, 3–4.
- 25 Ibid., 3–4.
- 26 “Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space, and Under Water,” Department of State, <https://2009-2017.state.gov/t/avc/trty/199116.htm#signatory>.
- 27 Andrea Shalal-Esa, “China Jamming Test Sparks U.S. Satellite Concerns,” Reuters, October 5, 2006, as quoted in Yousaf Butt, “Effects of Chinese Laser Ranging on Imaging Satellites,” *Science & Global Security* 17, no. 1 (2009): 20–35, <http://scienceandglobalsecurity.org/archive/sgs17butt.pdf>.
- 28 Harrison et al., *Space Threat Assessment*, 24–25.
- 29 Brian Garino and Jane Gibson, “Space System Threats,” in AU-18 Space Primer (Maxwell Air Force Base, AL: Air University Press, September 2009), 277, http://space.au.af.mil/au-18-2009/au-18_chap21.pdf.
- 30 Richard B. Langley et al., “Innovation: GNSS Spoofing Detection,” GPS World, June 1, 2013, <http://gpsworld.com/innovation-gnss-spoofing-detection-correlating-carrier-phase-with-ra-pid-antenna-motion/>.
- 31 Harrison et al., *Space Threat Assessment*, 38–39.
- 32 Tzvi Joffe, “U.S. warns of GPS interference, communications spoofing in Persian Gulf,” *Jerusalem Post*, August 8, 2019, <https://www.jpost.com/middle-east/us-warns-of-gps-interference-communications-spoofing-in-persian-gulf-597998>.
- 33 Sui-Lee Wee, “China Denies It Is behind Hacking of U.S. Satellites,” Reuters, October 31, 2011, <https://www.reuters.com/article/us-china-us-hacking/china-denies-it-is-behind-hacking-of-u-s-satellites-idUSTRE79U1YI20111031>.
- 34 U.S.-China Economic and Security Review Commission, *2015 Report to Congress* (Washington, DC: 2015), 296, https://www.uscc.gov/sites/default/files/annual_reports/2015%20Annual%20Report%20to%20Congress.PDF.
- 35 Office of the Inspector General, *Cybersecurity Management and Oversight at the Jet Propulsion Laboratory* (Washington, DC: NASA, 2019), 8–9, <https://oig.nasa.gov/docs/IG-19-022.pdf>.
- 36 U.S. Joint Chiefs of Staff, Joint Publication 3-14: Space Operations, I-2.
- 37 U.S. Air Force, *Annex 3-14 Counterspace Operations* (Maxwell Air Force Base, AL: August 2018), 10, https://www.doctrine.af.mil/Portals/61/documents/Annex_3-14/Annex-3-14-Counterspace-Ops.pdf; and John W. Raymond, Chief of Space Operations’ Planning Guidance (Washington, DC: November 2020), 36, <https://media.defense.gov/2020/>



Nov/09/2002531998/-1/-1/0/CSO%20PLANNING%20GUIDANCE.PDF.

- 38 U.S. Air Force, *Annex 3-14 Counterspace Operations*, 9.
- 39 Florence Parly, “Presentation of the Defense Space Strategy,” *SatelliteObservation.net*, July 25, 2019, English translation from: <https://satelliteobservation.net/2019/07/27/frances-new-space-defense-strategy/>.
- 40 U.S. Joint Chiefs of Staff, *Joint Publication 3-14: Space Operations*, I-8.
- 41 Tom Risen, “Disaggregation,” *Aerospace America*, April 17, 2017, <https://aerospaceamerica.aiaa.org/features/disaggregation/>.
- 42 Department of the Air Force, *Department of Defense Fiscal Year (FY) 2021 Budget Estimates: Air Force: Research, Development, Test & Evaluation, Space Force* (Washington, DC: Department of Defense, February 2020), 75–90, https://www.saffm.hq.af.mil/Portals/84/documents/FY21/RDTE_/FY21%20Space%20Force%20Research%20Development%20Test%20and%20Evaluation.pdf?ver=2020-02-11-083608-887.
- 43 Dorminey and Gomez, eds., *America’s Nuclear Crossroads*, 29-36.
- 44 Ellen Pawlikowski, Doug Loverro, and Tom Cristler, “Disruptive Challenges, New Opportunities, and New Strategies,” *Strategic Studies Quarterly*, Spring 2012, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-06_Issue-1/Pawlikowski.pdf.
- 45 Office of the Assistant Secretary of Defense for Homeland Defense & Global Security, *Space Domain Mission Assurance: A Resilience Taxonomy* (Washington, DC: Department of Defense, September 2015), 6–7, <https://policy.defense.gov/Portals/11/Space%20Policy/ResilienceTaxonomyWhitePaperFinal.pdf?ver=2016-12-27-131828-623>.
- 46 Risen, “Disaggregation.”
- 47 U.S. Joint Chiefs of Staff, *Joint Publication 3-14: Space Operations*, I-8.
- 48 *Ibid.*, I-9.
- 49 Winfred B. Hirschmann, “Profit from the Learning Curve,” *Harvard Business Review*, January 1964, <https://hbr.org/1964/01/profit-from-the-learning-curve>.
- 50 Sandra Erwin, “Boeing to deliver WGS-11 communications satellite to U.S. Air Force by 2024,” *Space News*, December 26, 2019, <https://spacenews.com/boeing-to-deliver-wgs-11-communications-satellite-to-u-s-air-force-by-2024/>.
- 51 Department of Defense, *Department of Defense Fiscal Year (FY) 2021 Budget Estimates: Space Development Agency: Research, Development, Test & Evaluation, Defense-Wide*, Vol. 5 (Washington, DC: February 2020), 1, https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2021/budget_justification/pdfs/03_RDT_and_E/SDA_PB2021.pdf.
- 52 Office of the Assistant Secretary of Defense for Homeland Defense & Global Security, *Space Domain Mission Assurance*, 7.
- 53 “Beidou Global Navigation Satellite System,” Information and Analysis Center for Position, Navigation, and Timing, n.d., <https://www.glonass-iac.ru/en/guide/beidou.php>.
- 54 David Wright, Laura Grego, and Lisbeth Gronlund, *The Physics of Space Security* (Cambridge, MA: American Academy of Arts and Sciences, 2005), 114, 133, <https://aerospace.csis.org/wp-content/uploads/2019/06/physics-space-security.pdf>.
- 55 Sandra Erwin, “Air Force: SSA is no more; it’s ‘Space Domain Awareness,’” *Space News*, November 14, 2019, <https://spacenews.com/air-force-ssa-is-no-more-its-space-domain-awareness/>.
- 56 Sandra Erwin, “Space Force needs sensors to distinguish weapons from benign objects,” *Space News*, January 6, 2021, <https://spacenews.com/space-force-needs-sensors-to-distinguish-weapons-from-benign-objects/>.
- 57 “Geosynchronous Space Situational Awareness Program,” Air Force Space Command, June 22, 2017, <https://www.afspc.af.mil/About-Us/Fact-Sheets/Article/730802/geosynchronous-space-situational-awareness-program-gssap/>.
- 58 Mark Dickinson, “A Space Data Association Focus: The current state of Space Situation-



- al Awareness (SSA)," *Sat Magazine*, January 2019, <http://www.satmagazine.com/story.php?number=1895054050>.
- 59 Sydney J. Freeberg, Jr., "US Jammed Own Satellites 261 Times; What If Enemy Did?," *Breaking Defense*, December 2, 2015, <https://breakingdefense.com/2015/12/us-jammed-own-satellites-261-times-in-2015-what-if-an-enemy-tried/>.
 - 60 "Technology," *HawkEye360*, <https://www.he360.com/technology/>.
 - 61 David S. F. Portree, "Starfish and Apollo (1962)," *Wired*, March 21, 2012, <https://www.wired.com/2012/03/starfishandapollo-1962/>.
 - 62 Wright, Grego, and Gronlund, *The Physics of Space Security*, 128.
 - 63 *Ibid.*, 118.
 - 64 Mosa Ali Abu-Rgheff, *Introduction to CDMA Wireless Communications* (Cambridge, MA: Academic Press, 2007), p 167-169.
 - 65 Todd Harrison, *The Future of MILSATCOM* (Washington, DC: CSBA, 2013), 25-26, <https://csbaonline.org/uploads/documents/Future-of-MILSATCOM-web.pdf>.
 - 66 William C. Cummings, "An adaptive nulling antenna for military satellite communications," *Lincoln Laboratory Journal* 5, no. 2 (1992), 174, <https://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=A294DF289CCE0FA300F262BD361D77C2?doi=10.1.1.230.8496&rep=rep1&type=pdf>.
 - 67 Patrick Howell O'Neill, "The quest for quantum-proof encryption just made a leap forward," *MIT Technology Review*, August 3, 2020, <https://www.technologyreview.com/2020/08/03/1005891/search-for-quantum-proof-encryption-computing-nist/>.
 - 68 U.S. Joint Chiefs of Staff, *Joint Publication 3-14: Space Operations*, I-8.
 - 69 James Mattis, *Summary of the National Defense Strategy of the United States of America* (Washington, DC: Department of Defense, 2018), 6, <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.
 - 70 Wright, Grego, and Gronlund, *The Physics of Space Security*, 46.
 - 71 Rebecca Reesman and James R. Wilson, *The Physics of Space War: How Orbital Dynamics Constrain Space-to-Space Engagements* (El Segundo, CA: Aerospace Corporation, October 2020), 11-14, https://aerospace.org/sites/default/files/2020-10/Reesman_PhysicsWarSpace_20201001.pdf.
 - 72 U.S. Congress, Office of Technology Assessment, *Anti-Satellite Weapons, Countermeasures, and Arms Control* (Washington, DC: U.S. Government Printing Office, September 1985), 81, <https://aerospace.csis.org/wp-content/uploads/2018/09/OTA-Report-on-ASAT-Weapons-and-Countermeasures-1985.pdf>.
 - 73 Jason A. Reiter, David B. Spencer, and Richard Linares, *Spacecraft Stealth Through Orbit-Perturbing Maneuvers Using Reinforcement Learning* (Reston, VA: American Institute of Aeronautics and Astronautics, January 2020), <https://arc.aiaa.org/doi/10.2514/6.2020-0461>.
 - 74 U.S. Joint Chiefs of Staff, *Joint Publication 3-14: Space Operations*, I-9.
 - 75 "MALD Decoy," Raytheon, n.d., <https://www.raytheonmissilesanddefense.com/capabilities/products/mald-decoy>.
 - 76 Walker Mills, "A Tool for Deception: The Urgent Need for Em Decoys," War Room, U.S. Army War College, February 27, 2020, <https://warroom.armywarcollege.edu/articles/tactical-decoys/>.
 - 77 U.S. Space Force, *Spacepower: Doctrine for Space Forces* (Washington, DC: August 2020), 36, https://www.spaceforce.mil/Portals/1/Space%20Capstone%20Publication_10%20Aug%202020.pdf.
 - 78 For more on cross-domain deterrence, see: King Mallory, "New Challenges in Cross-Domain Deterrence," RAND, 2018, https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE259/RAND_PE259.pdf.
 - 79 "Northrop Grumman to install LAIRCM laser missile defense systems aboard U.S. large



military aircraft,” Military and Aerospace Electronics, May 6, 2020, <https://www.military-aerospace.com/sensors/article/14175295/laser-missile-defense-large-aircraft>.

- 80 Florence Parly, “Presentation of the Defense Space Strategy.”
- 81 Thomas G. Roberts, “What Can 24 Satellites Do for U.S. Missile Defense?,” CSIS, *CSIS Brief*, October 2018, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/181018_Roberts_24SatellitesMissileDefense.pdf?9qnhsjRijr4PmHWE3N-sA0hshW2KIBJp6.
- 82 Thomas G. Roberts, “Bad Idea: Space-Based Missile Interceptors,” CSIS Defense360, December 19, 2017, <https://defense360.csis.org/bad-idea-brilliant-pebbles-thomas-roberts/>.
- 83 Caleb Henry, “Northrop Grumman’s MEV-1 servicer docks with Intelsat satellite,” Space News, February 26, 2020, <https://spacenews.com/northrop-grummans-mev-1-servicer-docks-with-intelsat-satellite/>.
- 84 Tereza Pultarova, “Watch a Satellite Fire a Harpoon in Space in Wild Debris-Catching Test,” Space.com, February 18, 2019, <https://www.space.com/space-junk-harpoon-removedebris-satellite-video.html>.
- 85 This is likely to remain the case until there is substantial economic activity and human presence in space that is somewhat independent of Earth. For example, large-scale mining of in-space resources and the use of those resources to support other activities in space, such as human colonies on other celestial bodies, could give nations a reason to protect or attack space lines of commerce to achieve economic and political objectives in space rather than on Earth. Human history has shown that wherever commerce goes, conflict is likely to follow.
- 86 See Christian Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare*.
- 87 Kaitlyn Johnson, “A Balance of Instability: Effects of Direct-Ascent Anti-Satellite Weapons Ban on Nuclear Stability,” Defense360, CSIS, October 21, 2020, 9–10, http://defense360.csis.org/wp-content/uploads/2020/10/2Kaitlyn_A-Balance-of-Instability.pdf.
- 88 For a more complete discussion of Space Domain Mission Assurance, see: Office of the Assistant Secretary of Defense for Homeland Defense & Global Security, Space Domain Mission Assurance.
- 89 The AM7 is a European built EUROSTAR Bus by Airbus with a Thales Alenia Payload, see <https://eng.rscg.ru/space/seriya-ekspress-am/ekspress-am7/>.
- 90 Due to continued delays in fielding M-Code GPS receivers, many U.S. forces and nearly all allied forces are still reliant on P(Y) or SASSM receivers.
- 91 Dee Ann Divis, “FCC Raises Questions about U.S. Access to Non-GPS GNSS,” Inside GNSS, January 16, 2015, <https://insidegnss.com/fcc-raises-questions-about-u-s-access-to-non-gps-gnss/>.
- 92 Multiple satellites may be located at the same orbital mode if their frequency plans are coordinated. DirecTV has maintained three satellites in this location since 2014.



CSIS | CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES

1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

**ROWMAN &
LITTLEFIELD**

Lanham · Boulder · New York · London

4501 Forbes Boulevard
Lanham, MD 20706
301-459-3366 | www.rowman.com