SPACE THREAT ASSESSMENT 2023

Authors
KARI A. BINGEN
KAITLYN JOHNSON
MAKENA YOUNG

Foreword
JOHN W. “JAY” RAYMOND
SPACE THREAT ASSESSMENT 2023

Authors
KARI A. BINGEN
KAITLYN JOHNSON
MAKENA YOUNG

Foreword
JOHN W. "JAY" RAYMOND

A REPORT OF THE
CSIS AEROSPACE SECURITY PROJECT
ABOUT CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, non-profit 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).

© 2023 by the Center for Strategic and International Studies. All rights reserved.

ABOUT ASP

The Aerospace Security Project (ASP) is the leading source of analysis and expertise on the policy and technology issues shaping the future of aerospace security. Part of the International Security Program at CSIS, ASP is led by Senior Fellow Kari A. Bingen. Learn more at aerospace.csis.org.

ACKNOWLEDGMENTS

The Aerospace Security Project would like to thank Slingshot Aerospace, Spire Global, and COMSPOC for their contribution of data and analysis. Finally, many thanks to Yash Bajaj, Patrick Fish, Jennifer Jun, Todd Harrison, Jeeah Lee, Phillip Meylan, Sarah Mineiro, Thomas G. Roberts, Katherine Stark, and William Taylor for their support in the research and publication process.

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.

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

1 FOREWORD

2 INTRODUCTION

3 TYPES OF COUNTERSPACE WEAPONS
   4 Kinetic Physical
   4 Non-kinetic Physical
   4 Electronic
   5 Cyber

8 CHINA

12 RUSSIA
   16 Featured Analysis: Russia’s War on Ukraine

21 INDIA

24 IRAN

27 NORTH KOREA

30 OTHERS
   30 Australia
   31 France
   31 Israel
   31 Japan
   32 South Korea
   32 United Kingdom
   32 Non-state Actors

33 WHAT TO WATCH

37 CONCLUSION

38 ABOUT THE AUTHORS
OF THE STRATEGIC ENVIRONMENT
is the most complex in the history of our nation—with China, our
pace challenge, and Russia, an acute threat, both challenging
the world order that has been in place and has secured peace since
the end of World War II.

Space is central to this complexity. Not only does space underpin all instru-
ments of our national power, but access to and freedom to maneuver in the
domain are foundational to the United States’ status as a great power. This
sixth edition of the Space Threat Assessment describes a domain undergo-
ing a significant and rapid transformation. The number of objects in space
continues to soar, the value of the global space economy is at an all-time
high, and, unfortunately, the threat to the domain is real and concerning
today. Over the past year and a half, there has been regular testing and use
of reversible non-destructive capabilities as well as a destructive test that
created a debris field, jeopardizing safe operations and indicating that the
domain will continue to become more contested.

Two significant threats face the United States with this rapid change in the
domain. First, China and Russia are developing and integrating space capa-
bilities that will afford them the same advantages the United States currently
enjoy, placing U.S. forces at great risk. Second, they are developing a robust
spectrum of offensive capabilities to deny the United States and its partners,
including commercial space companies, access to the domain.

This edition of the Space Threat Assessment includes a dedicated section on
the Russia-Ukraine war. Commercial space capabilities are making a significant
contribution to the fight and have provided Ukraine access to space that they
do not have organically. Commercial space has served as a great equalizer,
allowing Ukrainian forces to have the necessary intelligence, surveillance,
and reconnaissance and command and control to better understand Russian
force disposition, communicate and stay connected globally, and strike with
precision. Therefore, it is not surprising that Russia has tried to deny access
to these commercial capabilities largely through jamming and cyberattacks.

As some have suggested, the Russia-Ukraine war is “the first commercial
space war,” and it has highlighted areas where the use of commercial space
capabilities has advanced ahead of policy, strategy, and concepts of opera-
tions. This assessment is important to having a better understanding of the
threats faced in, to, and from the domain and should be a valuable source of
information to inform policymakers to be better prepared for future conflicts.

While there are significant challenges, the space domain offers even more
opportunities. The United States remains the world leader in space. U.S.
allies, partners, and the commercial space sector provide great advantage.
With strengthened leadership in the domain, the United States must continue
to define safe and professional behavior in space to its advantage, seek in-
creased transparency, strengthen our partnerships, and develop capabilities
necessary to deter conflict—and if deterrence were to fail, to win.

GENERAL JOHN W. “JAY” RAYMOND
U.S. SPACE FORCE, RETIRED
Former Chief of Space Operations
INTRODUCTION

WELCOME TO THE SIXTH EDITION of *Space Threat Assessment* by the Aerospace Security Project at the Center for Strategic and International Studies (CSIS). This resource for policymakers and the public leverages open-source information to assess key developments in foreign counterspace weapons. Drawing on six years of collected data and analyses, this series describes trends in the development, testing, and use of counterspace weapons and enables readers to develop a deeper understanding of threats to U.S. national security interests in space.

The past year was dominated by the Russian invasion of Ukraine, where space capabilities, including commercial satellites, played a highly visible and compelling role in Ukraine’s resistance to the invasion. Communications and imagery satellites have been used to connect Ukrainian troops across the battlefield, track Russian military movements, and map humanitarian corridors. As space capabilities continue to demonstrate their utility, from peacetime to conflict, it should come as no surprise that adversaries seek to block their use. Thus, this year’s featured analysis provides an in-depth look at Russia’s battlefield employment of counterspace weapons.

Russia, China, Iran, and others continue to pursue a wide range of space and counterspace activities, enabled by national policies, prioritized resources, and investments in supporting infrastructure. As General B. Chance Saltzman, the chief of space operations of the U.S. Space Force, noted in February 2023, “We are seeing a whole mix of weapons being produced by our strategic competitors.” Not only are these counterspace weapons in development and testing, but some have progressed to production and fielding in operational units. Such weapons could create disastrous effects for an array of national security, civil, and commercial users, especially if destructive weapons are employed that create orbital debris and render large swaths of popular orbits unusable.

The impacts of counterspace weapons use are no longer limited to military users alone. Harm to commercial and international space assets will also reverberate across the expanding space economy. According to the Space Foundation, 90 countries operate in space. The value of the global space economy was $469 billion in 2021, with other analyses projecting it will increase to over $1.25 trillion in annual revenue by 2030. While over 5,400 satellites are in-orbit today, more than 24,500 satellites are anticipated to be launched in the next 10 years (2022–2031), over 70 percent of which will be commercial.

This iteration of the *Space Threat Assessment* provides a framework that describes different types of counterspace weapons and a highlight of the main countries being tracked—China, Russia, India, Iran, North Korea, and others. The country sections include an overview of military space organizations, launch and satellite capabilities, and a brief review of counterspace developments. In addition, the report identifies key counterspace events in 2022, analyzes them in more detail, and provides a more comprehensive list of all notable counterspace activities and developments over the past year (January 2022–February 2023). The conclusion includes an analysis of notable trends and expectations for the coming year.

For more detail on past counterspace weapons tests, including historical tests by the United States and the Soviet Union, please review the prior *Space Threat Assessments* (editions 2018–2022) or visit the project’s interactive timeline at [https://aerospace.csis.org/counterspace-timeline/](https://aerospace.csis.org/counterspace-timeline/).
SPACE IS AN INCREASINGLY IMPORTANT ENABLER of economic and military power. The strategic importance of space has led some nations to build arsenals of counterspace weapons to disrupt, degrade, or destroy space systems and hold at risk the ability of others to use the space domain. However, the strategic importance of space has also spurred renewed efforts to deter or mitigate conflict and protect the domain for peaceful uses. For example, the U.S. Space Force’s capstone publication on spacepower notes that “military space forces should make every effort to promote responsible norms of behavior that perpetuate space as a safe and open environment in accordance with the Laws of Armed Conflict, the Outer Space Treaty, and international law, as well as U.S. Government and DoD policy.” Similarly, the 2022 North Atlantic Treaty Organization’s (NATO) Strategic Concept, adopted by NATO heads of state and government in June 2022, expresses the alliance’s commitment to upholding international law, promoting responsible behavior in space, and boosting the resilience of space capabilities. It further articulates that “secure use of and unfettered access to space” are key to effective deterrence and defense.

Counterspace weapons, particularly those that produce orbital debris, pose a serious risk to the space environment and the ability of all nations to use the space domain for prosperity and security. This chapter provides an overview of different types of counterspace weapons, drawing on previous CSIS work to taxonomize them. Counterspace weapons vary significantly in the types of effects they create, how they are deployed, their detectability, their ability to be attributed to a source, and the level of technology and resources needed for their development and fielding. This report categorizes counterspace weapons into four broad groups of capabilities: kinetic physical, non-kinetic physical, electronic, and cyber.
**KINETIC PHYSICAL**

**KINETIC PHYSICAL COUNTERSPACE** weapons attempt to strike directly or detonate a warhead near a satellite or ground station. The three main forms of kinetic physical attack are direct-ascent anti-satellite (ASAT) weapons, co-orbital ASAT weapons, and ground station attacks. Direct-ascent ASAT weapons are launched from Earth on a suborbital trajectory to strike a satellite in orbit, while co-orbital ASAT weapons are first placed into orbit and then later maneuvered into or near their intended target in orbit. These maneuvers are commonly known as rendezvous and proximity operations (RPOs). Attacks on ground stations are targeted at the terrestrial sites responsible for the command and control of satellites or the relay of satellite mission data to users. Such a ground station attack has the benefit of affecting many satellites in a constellation (that communicate with the ground station) rather than requiring multiple weapons to target individual satellites.

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 carry the potential for the direct 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 (ISS) in low Earth orbit (LEO). To date, no country has conducted a kinetic physical attack against another country’s satellite, but four countries—the United States, Russia, China, and India—have successfully tested direct-ascent ASAT weapons against their own satellites. The Soviet Union also tested co-orbital kinetic ASAT weapons as early as the 1960s.

**NON-KINETIC PHYSICAL**

**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 or 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 and an electromagnetic pulse (EMP) with indiscriminate effects on satellites in affected orbits. Non-kinetic attacks operate at the speed of light and, in some cases, can be less visible to third-party observers and more difficult to attribute. 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. A laser can only 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. 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. 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.

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 EMP, 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, though this does not include China or North Korea.¹⁰

**ELECTRONIC**

**ELECTRONIC COUNTERSPACE** weapons target the electromagnetic spectrum through which space systems transmit and receive data. Jamming devices interfere with communications to or from satellites by generating noise in the same radio frequency.
COUNTERSPACE WEAPONS

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 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.

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 communications can return to normal once the jamming signal is removed. Through a type of spoofing called “meaconing,” even encrypted military P(Y) GPS signal can be spoofed. Meaconing does not require cracking the encryption because it merely rebroadcasts a time-delayed copy of the original signal without decrypting it or altering the data. The technology needed to jam and spoof many types of satellite signals is commercially available and inexpensive, making it relatively easy to proliferate among state and non-state actors.

CYBER

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 or commands 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 issuing commands that cause it to expend propellant or 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, when launching an attack.

UPLINK JAMMER

DOWNLINK JAMMER

Illustration
Cyberattacks can be used to take control of a satellite and damage or destroy it.

Illustration
Uplink and downlink jamming are two forms of electronic counterspace attack.
# Table 1
## TYPES OF COUNTERSPACE WEAPONS

<table>
<thead>
<tr>
<th>Types of Attack</th>
<th>Kinetic Physical</th>
<th>Non-kinetic Physical</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ground Station Attack</td>
<td>Direct-Ascent ASAT</td>
<td>Co-orbital ASAT</td>
</tr>
<tr>
<td>High Altitude Nuclear Detonation</td>
<td>High-Powered Laser</td>
<td>Laser Dazzling or Blinding</td>
</tr>
<tr>
<td>Launch site can be attributed</td>
<td>Can be attributed by tracking previously known orbit</td>
<td>Launch site can be attributed</td>
</tr>
<tr>
<td>Limited attribution</td>
<td>Clear attribution of the laser’s location at the time of attack</td>
<td>Limited attribution</td>
</tr>
<tr>
<td>Irreversible</td>
<td>Irreversible</td>
<td>irreversible or reversible depending on capabilities</td>
</tr>
<tr>
<td>Only satellite operator will be aware</td>
<td>Only satellite operator will be aware</td>
<td>Only satellite operator will be aware</td>
</tr>
<tr>
<td>May or may not be publicly known</td>
<td>Publicly known</td>
<td>Publicly known</td>
</tr>
<tr>
<td>Near real-time confirmation of success</td>
<td>Near real-time confirmation of success</td>
<td>Near real-time confirmation of success</td>
</tr>
<tr>
<td>Limited confirmation of success if satellite begins to drift uncontrolled</td>
<td>No confirmation of success</td>
<td>Limited confirmation of success if satellite begins to drift uncontrolled</td>
</tr>
<tr>
<td>May or may not produce orbital debris</td>
<td>Higher radiation levels in orbit would persist for months or years</td>
<td>Could leave target satellite disabled and uncontrollable</td>
</tr>
<tr>
<td>Could leave target satellite disabled and uncontrollable</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

**Attributes:**
- **Variable attribution, depending on mode of attack**
- **Publicly known depending on trajectory**
- **May or may not be publicly known**
- **Near real-time confirmation of success**
- **May or may not control multiple satellites, potential for loss of life**
- **Higher radiation levels in orbit would persist for months or years**
<table>
<thead>
<tr>
<th>Types of Attack</th>
<th>Electronic</th>
<th>Cyber</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Uplink Jamming</strong></td>
<td>Modest attribution depending on mode of attack</td>
<td>Limited or uncertain attribution</td>
</tr>
<tr>
<td><strong>Downlink Jamming</strong></td>
<td>Modest attribution depending on mode of attack</td>
<td>Limited or uncertain attribution</td>
</tr>
<tr>
<td><strong>Spoofing</strong></td>
<td>Modest attribution depending on mode of attack</td>
<td>Limited or uncertain attribution</td>
</tr>
<tr>
<td><strong>Data Intercept or Monitoring</strong></td>
<td>Data Corruption</td>
<td>Seizure of Control</td>
</tr>
<tr>
<td><strong>Data Corruption</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Seizure of Control</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Attribution</strong></th>
<th><strong>Reversibility</strong></th>
<th><strong>Awareness</strong></th>
<th><strong>Attacker Damage Assessment</strong></th>
<th><strong>Collateral Damage</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Modest attribution depending on mode of attack</td>
<td>Reversible</td>
<td>Satellite operator will be aware; may or may not be known to the public</td>
<td>No confirmation of success</td>
<td>Only disrupts the signals targeted and possible adjacent frequencies</td>
</tr>
<tr>
<td>Modest attribution depending on mode of attack</td>
<td>Reversible</td>
<td>May or may not be known to the public</td>
<td>Limited confirmation of success if monitoring of the local RF environment is possible</td>
<td>Only disrupts the signals targeted and possible adjacent frequencies</td>
</tr>
<tr>
<td>Modest attribution depending on mode of attack</td>
<td>Reversible</td>
<td>May or may not be known to the public</td>
<td>Limited confirmation of success if effects are visible</td>
<td>Only corrupts the specific RF signals targeted</td>
</tr>
<tr>
<td>Limited or uncertain attribution</td>
<td>Reversible</td>
<td>Satellite operator will be aware; may or may not be known to the public</td>
<td>Near real-time confirmation of success</td>
<td>None</td>
</tr>
<tr>
<td>Limited or uncertain attribution</td>
<td>Reversible</td>
<td>Satellite operator will be aware; may or may not be known to the public</td>
<td>Near real-time confirmation of success</td>
<td>None</td>
</tr>
<tr>
<td>Limited or uncertain attribution</td>
<td>Irreversible or reversible, depending on mode of attack</td>
<td>Satellite operator will be aware; may or may not be known to the public</td>
<td>Near real-time confirmation of success</td>
<td>Could leave target satellite disabled and uncontrollable</td>
</tr>
</tbody>
</table>

**CSIS AEROSPACE SECURITY PROJECT RESEARCH AND ANALYSIS**
China continues to make progress toward its goal of becoming the world leader in space. Over the past year, China has continued to grow its space and counterspace assets, maintaining its status as the second-most-capable space nation after the United States. To enable these capabilities, China operates four spaceports and a family of Long March space launch vehicles (SLVs) that can deliver a wide range of satellites to different orbital altitudes. In 2022, China conducted 64 space launches, including two space launch failures. The successful launches resulted in over 150 satellites successfully placed into orbit and the launch of one orbital and one suborbital spaceplane.

Civil, intelligence, and military space capabilities are a priority for China as it continues to invest in and plan for greater use and access to space in the coming decade. In November 2022, China completed the construction of the Tiangong space station, which is now operational. Beijing has released two white papers on space activities, in 2016 and 2021, which not only outline a vision for future space activities but also integrate space into other strategic global initiatives.
SPACE ORGANIZATION

While China has separate organizations charged with managing its civil and military space activities, much of the technology for both civil and military space capabilities is produced by the same state-owned enterprises. The line between commercial and governmental endeavors is often blurred by Beijing’s military-civilian fusion policy, which encourages such enterprises to acquire and divert cutting-edge technologies, including space technology, to achieve both economic and military dominance.  

The China National Space Administration (CNSA) leads all civil space missions. The CNSA falls within the purview of the State Council’s State Administration for Science, Technology, and Industry for National Defense. China’s space program primarily contracts through the China Aerospace Science and Technology Corporation, a state-owned enterprise with many sectors that researches and develops SLVs, spacecraft, missile systems (including intercontinental ballistic missiles), and supporting ground equipment. Finally, the China Aerospace Science and Industry Corporation is another state-owned enterprise which specializes in space technologies.

The military organization for space capabilities, the Strategic Support Force (SSF), sits alongside other information-centric domains, such as cyber, within China’s People’s Liberation Army (PLA). Founded in 2015, the SSF manages space warfare, space launch, and the acquisition and operation of satellites. Within the SSF, the Space Systems Department and Network Systems Department divide responsibilities and act as co-equal semi-independent branches, with the former managing space and counterspace capabilities and the latter leading the cyber, electronic, and psychological warfare mission areas.

SPACE LAUNCH CAPABILITIES

China broke its launch record in 2022, sur-passing its previous record of 55 launches set in 2021. The vast majority of these missions were launched on the Long March SLV family of rockets. The Long March-2 (variants C, D, and F), -3B, -4C, -5, -5B, -6, -7, -8, and -11 rockets provide light-, medium-, and heavy-lift capability to LEO and geostationary orbit (GEO). Some are capable of launching from a sea-based platform, but most launch from traditional ground-based launch pads. Newer Long March vehicles are being developed, including the Long March-9.

These SLVs are typically launched from one of four sites in China. The Jiuquan Satellite Launch Center, located in Inner Mongolia, was founded in 1958 and is the country’s oldest space launch facility. This is the most popular launch site and has been the site of the majority of the country’s space tests and launches, including the launch of China’s first satellite in 1970, and the first international payload launched from the country in 1992. The Taiyuan Satellite Launch Center, located in Wuzhai, Shanxi, is another popular launch site with a history of space and ballistic missile launches dating back to 1968. The Taiyuan Satellite Launch Center also has test and assembly capabilities on campus and launches vehicles too large for the Jiuquan Satellite Launch Center. The other two Chinese launch sites were both built to support human, interplanetary, and lunar missions. Located in the Sichuan region, the Xichang Satellite Launch Center (Songlin) was finalized in 1984, but because of its close proximity to populated areas has now become a backup launch site to China’s most recent addition, the Wenchang Satellite Launch Center.

The coastal Wenchang Satellite Launch Center, located on the island province of Hainan in the South China Sea, has hosted 16 launches since opening in 2014. Officials have announced plans to further develop Wenchang as a commercial spaceport with satellite assembly, testing, and data centers on-site. In addition to these launch sites, China is capable of launching from mobile platforms in the Yellow Sea.

There has been a shift in the last decade for the Chinese commercial industry. In 2014, the Chinese government lifted a restrictive policy prohibiting the creation of commercial space launch companies and commercial launch technology, which has resulted in private and state investment into the commercial market. Today, the government may look to the commercial sector as an opportunity to replace China’s reliance on international companies or suppliers. Similar to trends in other dominant space-faring nations, many commercial companies are focusing on launch capabilities. The first commercial space launch from China is expected in the first months of 2023 from Beijing Tianbing Technology Co., Ltd., also known as Space Pioneer, which plans to launch a Tianlong-2 medium-lift vehicle from the Jiuquan Satellite Launch Center.
China’s Spaceplane Program

Spaceplane programs are often extremely secretive, and the Chinese program is no exception. Spaceplanes launch from traditional SLVs, spend their operational mission continuously orbiting the Earth, and re-enter the atmosphere and land like a traditional airplane. The U.S. Space Shuttle is a famous larger cousin of the spaceplanes in operation today.

In August 2022, China launched two different spaceplanes, one orbital and one suborbital, from the Jiuquan Satellite Launch Center. As is typical with many emerging Chinese space technologies, few details have surfaced about either vehicle.

The first test of a Chinese spaceplane was in September 2020 and was launched by a Long March 2F. That spaceplane traveled in LEO for two days, released an object capable of broadcasting transmissions, and concluded its test flight by landing in northwest China.

The second test of this vehicle launched on another Long March 2F on August 4, 2022. After a successful launch and almost two months in LEO, the spaceplane raised its orbit on October 23 before releasing an object. Although it is not clear from publicly available data when exactly the spaceplane released its object, the U.S. Space Force space tracking database recognized the object on October 31, 2022.

There have been few details released since, and a Google translation of reporting from state media has only indicated that the spaceplane will remain in orbit for “a period of time.”

As of March 16, 2023, the orbital spaceplane is still believed to be in LEO. Available images of the Chinese spaceplane show that it bears a resemblance to the United States’ X-37B spaceplane, which completed a sixth mission in November 2022, after spending 908 days in orbit, and shows a Chinese interest in matching U.S. capabilities.

China launched its suborbital spaceplane for a second time on August 26, 2022, following an initial test in September 2019 on a Long March 2D rocket. A statement from the China Aerospace Science and Technology Corporation confirmed that this launch vehicle was re-used, making it the country’s first successful demonstration of a reusable space launch capability. Reporting from China indicates a large amount of funding to be allocated to a suborbital transport project capable of carrying passengers. Though the suborbital spaceplane was confirmed to have landed, reports have not confirmed the duration or altitude of its flight. China is also developing a similar launching project, called the Tengyun project, which will incorporate a horizontal takeoff and landing capability to increase the ease and speed of space launches.

There are no indications that a spaceplane capability would act as a counterspace weapon, but because of the apparent capacity to release objects while in orbit, this could progress to a co-orbital ASAT capability.

SATELLITE CAPABILITIES

China maintains an extensive suite of satellite capabilities, including advanced positioning, navigation, and timing (PNT); satellite communications; intelligence, surveillance, and reconnaissance (ISR); missile warning; and space situational awareness. According to a 2022 U.S. Defense Intelligence Agency report, China doubled its number of satellites in orbit between 2019 and 2021, from 250 to 499, and surpassed all but the United States in the number of space startups receiving funding, drawing 16 percent of total global investment in these ventures.

Notable capabilities include the Beidou constellation, made of 35 PNT satellites, which acts as China’s alternative to GPS. Satellite capabilities such as Beidou are increasingly used as tools for the Digital Silk Road and Belt and Road Initiatives. Similarly, China has released plans for a 13,000-satellite constellation in LEO for broadband communications purposes. This would be the country’s answer to SpaceX’s Starlink network and would aim to serve customers across China and underdeveloped internet markets across the globe. In 2019, China introduced the Belt and Road Space Information Corridor to build out Chinese space applications and services in other nations. Just two years later, in its
2021 space white paper, Beijing commended the successes of the corridor, highlighting expanding satellite research and development infrastructure in Egypt, Pakistan, and Nigeria as examples. Chinese commercial companies continue to develop capabilities as well; in 2021, space-mining start-up OriginSpace launched a space debris cleanup prototype into LEO. The company claims this capability will be able to remove space debris, potentially with a net, though there are no reports of the satellite’s on-orbit tests or RPO activities.

COUNTERSPACE ASSESSMENT OVERVIEW

As China continues to develop and deploy a robust arsenal of space and counterspace capabilities, U.S. officials continue to view the country as a significant counterspace threat. China maintains a substantial kinetic ASAT capability, most notably demonstrated by a debris-creating 2007 test, as well as numerous subsequent non-intercept tests in the years since. Co-orbital technology demonstrations prove China’s ability to rendezvous with other satellites in GEO. While these are not counterspace weapons tests, they demonstrate capability that is necessary for a co-orbital counterspace attack. Non-kinetic counterspace weapons, such as high-powered lasers or microwaves, remain largely classified or are not publicly known to have been tested. However, in a 2021 threat report, the U.S. Office of the Director of National Intelligence indicated that China has ground-based lasers capable of blinding or damaging optical sensors on low-altitude satellites. Reporting from 2022 indicated that Chinese universities are also working on small laser devices capable of being mounted on a satellite, though this is not a current capability. China’s jamming and spoofing electronic warfare capabilities have been verified in use against space and non-space signals alike. Few Chinese cyberattacks on space systems have been recorded in the last five years, but China’s cyber capabilities in other domains form a solid foundation for potential cyber counterspace capabilities. 

China also maintains significant space surveillance capabilities, which are required to effectively target and employ their counterspace weapons. The country has maintained a fleet of space-tracking ships for years, which set sail for months-long space-tracking and monitoring missions. The ships are reportedly capable of monitoring missions including Beidou satellites and the Chang’e lunar missions. In November 2022, China unveiled the SLC-18 radar, which is reportedly designed to “search, detect, and track objects such as ballistic missiles and LEO satellites.” This may be an updated design to the previous JY-26 “Skywatch” long-range air surveillance system debuted in 2014. Global space surveillance capabilities are an additional component of the country’s Belt and Road Initiative. China has had success building space surveillance infrastructure, particularly ground stations, in countries around the world, including as far away as South America.

CHINA DOUBLED ITS NUMBER OF SATELLITES IN ORBIT BETWEEN 2019 AND 2021, FROM 250 TO 499.

Rendezvous and Proximity Operations

China has a long history of satellites capable of performing on-orbit RPOs, commonly in GEO. As reported in last year’s assessment, the Shijian 21 (SJ-21) was launched in October 2021 as an experimental space debris mitigation satellite, which separated from its upper stage apogee kick motor (AKM). SJ-21 performed RPO maneuvers around the AKM before moving to rendezvous with a defunct Beidou satellite, Compass G2. AKMs are additional power sources that help place a satellite into a specific orbit. Since GEO is a highly valued orbit, most AKMs in GEO are released in a manner such that they separate and put significant distance between the payload and the AKM, so as not to interfere with satellite operations in GEO. Previous reporting suggests that SJ-21 performed several RPOs around Compass G2 before docking and moving the defunct satellite into a GEO graveyard orbit, hundreds of kilometers above the traditional GEO belt.

Updated information showcases that SJ-21 took Compass G2 significantly higher than a typical graveyard orbit, which is highly unusual for a debris removal mission. Two additional Chinese rendezvous technology research satellites, SJ-12-01 and -02 were launched into GEO in early 2022. Soon after, the satellites engaged with a U.S. Geosynchronous Space Situational Awareness Program space surveillance satellite in a “cat-and-mouse game” spanning several days. Each time the U.S. satellite would approach either SJ-12 satellite, the Chinese satellites would quickly maneuver away. These activities have been corroborated by commercial company COMSPOC and highlight the RPO capabilities China has successfully developed and maintained in orbit.

China’s first successful orbital launch of 2023 was on January 6. Shijian 23 (SJ-23) launched on a Long March 7 from the Wenchang Satellite Launching Center. SJ-23 reached its GEO orbit on January 15 and one day later a second object appeared to be tracked—another suspected AKM.
As one of the three dominant national space actors, Russia retains substantial space capabilities and forces, many dating back to the Soviet Union. However, Moscow finds itself at an inflection point. Over the past year, Russia has continued to display less advanced space and counterspace capabilities than originally anticipated. Advanced counterspace weapons that were promised, such as the Peresvet and Sokol-Eshelon ground-based lasers, are nowhere to be seen on the battlefield despite Russian claims of their success. Furthermore, reports have surfaced that the Russian space industrial base is suffering from sanctions, an aging population, corruption, and bloat.

Nevertheless, in 2022, Russia used space capabilities and counterspace weapons more than ever before. Widespread reports of jamming throughout Eastern Europe have been attributed to Russia, as have several distinct attacks on commercial space architectures, such as Viasat and SpaceX’s Starlink system. Moreover, Moscow continues to play a “cat-and-mouse” game in orbit, using its satellites to shadow other nations’ satellites and creating confusion and concern about the intent of these actions.
SPACE ORGANIZATION

Military and civil space organizations remain mostly separate in Russia, with the Russian Aerospace Forces (VKS) leading military efforts and Roscosmos leading those on the civil side. Within the VKS, military space and counterspace capabilities fall within the Russian Space Forces, established in 2015. The Russian Space Forces’ mission includes space situational awareness, missile warning, space launch, satellite operations, and counterspace operations. Roscosmos leads on human spaceflight, the GLONASS PNT system, and international space partnerships.

SPACE LAUNCH CAPABILITIES

Space launch capabilities are a cornerstone for Russia's military and civilian space programs. Providing space launch via the Soyuz rocket—which has been in operation for over 50 years—has brought in significant revenue for Russia over the years through the sale of payload space or seats for astronauts. In fact, to maintain U.S. presence on the ISS between the 2011 decommissioning of the U.S. Space Shuttle and the 2020 launch of SpaceX's Dragon capsule to the ISS with two U.S. astronauts, Moscow carried 71 U.S. astronauts to the station at a cost of approximately $56 million per seat. In total, these launches cost the National Aeronautics and Space Administration (NASA) approximately $4 billion.

Russia successfully launched 22 times in 2022. This pace is slightly behind 2021 and pre-pandemic years. Notably, Russia lost significant international launch customers after its invasion of Ukraine in early 2022. For example, just before a scheduled launch in early 2022, Roscosmos demanded that OneWeb not use any of its satellites to support military activities. After receiving no such reassurances, Roscosmos took a Soyuz launch vehicle containing 36 OneWeb satellites off the launch pad on March 4, 2022. The 36 satellites remain in storage in Russia. Due to the seizure of their satellites and the invasion of Ukraine, OneWeb canceled all future launches through Russia.

After a partial failure of Russia's heavy-launch Angara 5 in December 2021, Russia's lighter launch vehicle, the Angara 1.2, successfully launched twice in 2022, carrying two undisclosed military satellites into LEO. However, both satellites de-orbited and burned up in the Earth’s atmosphere within two months. Angara 1.2 is expected to conduct an additional launch in late 2023.

Russia maintains three main launch sites: Baikonur Cosmodrome in Kazakhstan, Plesetsk Cosmodrome in the northwest of the country, and the Vostochny Cosmodrome in the east. Baikonur is typically used for cosmonaut launches to the ISS, while Plesetsk is used for many military space launches, including a November 2021 direct-ascent ASAT test. President Vladimir Putin visited the Vostochny Cosmodrome in April 2022 to celebrate Cosmonautics Day, a holiday commemorating Yuri Gagarin’s successful mission as the first human in space. Putin was accompanied by Belarusian president Alexander Lukashenko for bilateral meetings and a tour of the site. Once fully operational, Vostochny is expected to host 45 percent of all Russian launches, shifting significant work from Baikonur to the new domestic launch site. The 2023 Angara 1.2 launch is planned for Vostochny Cosmodrome.

SATELLITE CAPABILITIES

Russia maintains a fleet of highly capable satellites providing support to a variety of...
RUSSIA

civil and military missions, including human spaceflight, deep space exploration, missile warning, communications, command and control, ISR, and weather. While many of these capabilities were developed in the 1990s or early 2000s, some are being revitalized. A national PNT system called GLONASS has been operational since 1993 and provides navigation capabilities to the Russian military and civilians, much like the United States’ own GPS. Updates to GLONASS are ongoing, and three new GLONASS satellites were launched in 2022. Several ISR and communications satellites were also launched in 2022 to complement or restore existing constellations.

Russia’s Federal Space Program 2016-2025, a policy and budgetary plan for its space projects, set ambitious goals, including increased bandwidth for communications satellites, additional remote sensing satellites, upgrades to the Russian segment of the ISS, and the completion of the Vostochny Cosmodrome. However, since enacting this policy, Moscow’s space budgets have continued to shrink. Sanctions enacted after the 2014 invasion of Crimea have significantly hampered the Russian space industry. Furthermore, after Russia’s 2022 invasion of Ukraine, additional sanctions were imposed on the aerospace industry by the United States and its allies, and joint projects were suspended by Russia’s international partners, such as the ExoMars rover mission with the European Space Agency. With shrinking budgets, expanding sanctions, and continued economic stagnation, Russia has focused its efforts on streamlining current space capabilities, specifically revitalizing Soviet-era programs and investing in dual-use space technologies—those with both military and civil uses. This strategy is a clear response to Russia’s burgeoning challenges in its national space enterprise. Many of these dual-use capabilities are discussed in the following section on Russian counterspace threats.

COUNTERSPACETHREAT ASSESSMENT OVERVIEW

Russia has a proven, well-rounded suite of counterspace weapons. Many of this year’s updates to Russia’s counterspace capabilities are found in the “Featured Analysis” section on page 16.

Kinetic Physical

In November 2021, Russia successfully tested a direct-ascent ASAT in LEO. The test partially destroyed a defunct Soviet-era satellite, Cosmos 1408, via a Nudol (PL-19) missile interceptor. Russia has tested the Nudol system almost yearly since 2014, but this was the first intercept on orbit that created space debris. Of the 1,783 pieces of orbital debris tracked from the test, only 661 were still in orbit as of September 2022. However, the remaining pieces are at a higher altitude, which mean the debris will remain in orbit until around 2033. Some of this debris is in a similar orbit to the ISS, which had to move three times in 2022 to avoid the debris.

In September 2018, a modified Russian MiG-31 fighter jet was photographed carrying an unidentified missile that was reportedly a “mock-up” of an air-launched ASAT weapon. Reports now suggest that this missile system is the Burevestnik. Little to no details are confirmed about the ASAT capability, but the capability is not new.

Co-orbital weapons are hard to identify and track in orbit. However, unusual or threatening behavior can provide insight into capabilities and intent. Russia has a long history of unusual and threatening behavior in both LEO and GEO and conducted similar activities in 2022. Luch, Russia’s well-known GEO inspector satellite, maneuvered several times in 2022 to closely approach and loiter near three different Intelsat communications satellites. For more information on Luch and its activities during Russia’s war on Ukraine, see page 20.

Non-kinetic Physical

It is possible that Russia has developed a new ground-based ASAT laser system, dubbed Kalina. Part of Russia’s Krona space surveillance station located in southwest Russia near the Black Sea, Kalina may be capable of dazzling or blinding satellites. It is unclear if this system is operational or capable of counterspace attacks, but it is a notable development for experts to monitor as progress on the facilities continue.

Electronic

Available open-source reporting indicates that GPS jamming is occurring around Mos-

Cosmos 2558’s Early Mission

In early August 2022, it was reported that Russian satellite Cosmos 2558 performed a close approach with USA 326, a U.S. National Reconnaissance Office (NRO) satellite, in LEO. Cosmos 2558 was likely close enough to image or collect signals intelligence from USA 326, but current reporting suggests it did not interfere with, deny, or degrade operations of the NRO satellite. With the speed at which satellites travel in LEO, the flyby of Cosmos 2558 would have happened relatively quickly and possibly within a couple of hours. General James H. Dickinson, commander of U.S. Space Command, spoke about this dangerously close approach to NBC News on August 9, 2022. A unique aspect of this mission was how early it occurred in the satellite’s lifetime. Cosmos 2558 was launched into space on August 1, 2022, and the close approach happened only three days later, on August 4. Following the approach, Cosmos 2558 adjusted its position in early September 2022 to stay within the same orbital plane as USA 326.
cow, and observers speculate that it is to protect the capital city from being targeted by Ukrainian drones. Russia has been installing jammers capable of denying GPS on domestic infrastructure, such as cell towers. The 2020 edition of this report highlighted how mobile GPS jamming vehicles accompany President Putin to ensure the leader’s personal safety and how GPS jamming may be used near the Kremlin. More information on how jamming has been used in Russia’s invasion of Ukraine can be found on page 18.

Cyber

Russia has demonstrated significant cyber capabilities, as showcased with its February 2022 Viasat hack. For more on this attack, please see “Featured Analysis” on page 17. Recent reports have emerged on another successful cyber intrusion against a U.S. commercial satellite communications provider. In November 2022, an analyst from the Cybersecurity and Infrastructure Security Agency (CISA) within the U.S. Department of Homeland Security stated at a conference that the Russian hacking group Fancy Bear successfully infiltrated a satellite communications network. The intruders were supposedly in the network for months before detection. Fancy Bear is a Russian state-sponsored advanced persistent threat group tracked by the U.S. government and confirmed to be part of the Russian General Staff Main Intelligence Directorate’s 85th Main Special Service Center.

Possible SAR Jamming

In June and July 2021, a defense blog reported on a potential electronic warfare attack on the European Space Agency’s Sentinel-1B synthetic aperture radar (SAR) imagery satellite. As of March 2023, this attack remains unconfirmed, but it is suspected that Russian forces were able to affect the European SAR satellite as it imaged Russian territory near the Sea of Azov and the Black Sea. After this report, the findings were highly questioned on Twitter, leaving it unclear if the satellite itself experienced SAR jamming or radar interference in the region. However, Moscow is reported to possess SAR-jamming capability, specifically its Krasukha-2/-4 mobile electronic warfare systems, which can jam both airborne and space-based radar systems. Possibly unrelated but worth mentioning is that Sentinel-1B suffered an anomaly in December 2021 that affected the satellite’s SAR antenna power system, leaving the satellite unable to collect SAR data. The European Space Agency declared “the capability of Sentinel-1B to support the mission is therefore considered lost,” and surmised that the probable cause of failure was the soldering processed used to repair a ceramic capacitor during the assembly and manufacturing of the satellite.
THE MOST SIGNIFICANT SPACE-RELATED DEVELOPMENTS IN 2022 center on Russia and its war on Ukraine. This edition of the Space Threat Assessment takes an in-depth look at Russian counterspace activities in this context. There has been an unparalleled level of transparency on the battlefield in Ukraine: sensitive intelligence was declassified to reveal Moscow’s plans and intentions, imagery showed the massing of Russian forces, and social media posts conveyed the war’s horrors up close. Space capabilities are aiding in this transparency and making an impactful contribution to this fight. Communications satellites are empowering Ukrainian forces and connecting the Ukrainian people with the outside world. Imagery satellites, some able to penetrate clouds and collect pictures at night, are watching the movement of Russian forces, mapping humanitarian evacuation routes, and collecting evidence of war crimes. Other satellites can detect and locate the sources of GPS interference, which is causing Ukrainian unmanned aerial vehicles (UAVs) to alter course. Some observers have described this war as the “first commercial space war” due to the prominence of Western space industry capabilities enabling Ukraine’s resistance.96

However, as with any advantage on the battlefield, adversaries quickly look for ways to erode that edge, and the same is true for space. This featured analysis details Russian employment of electronic warfare and cyberattacks against space systems, uncertainty on Russian use of laser weapons, and unusual behavior by a Russian inspector satellite in GEO. While the space lessons learned in Ukraine are still to be written, there may be insights to glean on Moscow’s space strategy and doctrine, and lessons for the United States to apply to threats in the Indo-Pacific.
MARCH 1, 2021

**Jamming**

Russian GPS jamming affects OSCE UAV in flight monitoring the Russia-Ukraine border.

OCTOBER 4, 2021

**Co-orbital**

Russian inspector satellite Luch maneuvers and lingers near Intelsat 33e for over 100 days.

NOVEMBER 15, 2021

**Direct-Ascent**

Russia conducts a direct-ascent ASAT test in LEO and destroys a defunct Soviet satellite.

JANUARY 23, 2022

**Co-orbital**

Luch maneuvers and lingers near Intelsat 39 for over 170 days.

FEBRUARY 24, 2022

**Cyber**

Russia successfully conducts a cyberattack against Viasat ground stations, cutting off satellite communications for the Ukrainian government.

MARCH 9, 2022

**Jamming**

Finnair reports several occurrences of GPS jamming when its commercial airliners near Kaliningrad.

MARCH 25, 2022

**Jamming**

Starlink engineers successfully resist Russian satellite communications jamming attempts by updating the system’s software.

SEPTEMBER 1, 2022

**Co-orbital**

Luch maneuvers and lingers near Intelsat 37 for about 145 days.

OCTOBER 27, 2022

**Diplomatic**

Konstantin Vorontsov, deputy director of Russian Foreign Ministry’s department of nonproliferation and arms, warns that “quasi-civilian infrastructure may become a legitimate target for retaliation.”

For a complete timeline of counterspace activities from 1959 to 2022, visit aerospace.csis.org/counterspacetimeline/.
RUSSIA

Russia’s attacks against space capabilities used by Ukraine are an example of how counterspace weapons can and will likely be used prior to and during future conflict.

JAMMING AND CYBERATTACKS

Months before the invasion, the Organization for Security and Cooperation in Europe (OSCE) was monitoring the Ukraine-Russia border using UAVs to perform overflight missions. The fleet of UAVs operated by the OSCE uses the unprotected civilian GPS signal to aid in their navigation. Throughout March and April 2021, over 60 percent of the OSCE’s UAV flights encountered GPS signal interference, including in areas near the OSCE base (approximately 25 kilometers from the contact line). These events were corroborated through RF signal sensing from a commercial space company which confirmed detection of GPS interference in the areas where OSCE UAVs were attempting to carry out the monitoring mission. The day before the invasion, on February 23, 2022, Ukrainian government sources stated that a long-range UAV experienced significant GPS interference, which caused a temporary loss of control of the aircraft. Open-source defense analysts from Janes assess that the long-range UAV was a Turkish Bayraktar (TB-2) drone operated by Ukraine and that the counter-UAV electronic warfare system was the Russian Krasukha-4. Russian employment of GPS-jamming devices has continued throughout the conflict.

Beyond electronic warfare against GPS systems, Russia moved to deny Ukrainian command and control systems enabled by commercial communications satellites. An hour before Russian troops invaded on February 24, 2022, Russia conducted a cyberattack to deny connectivity between the Viasat communications KA-SAT network and its thousands of ground terminals. The attack entered through a virtual private network and deployed wiper malware that crashed terrestrial modems via the satellite downlink. One of Viasat’s customers was the target: the Ukrainian government and military. However, the attack indiscriminately affected other Viasat users in Europe, including disabling about one-fifth of wind turbines and internet users across Central Europe. In light of the attack against Viasat, the U.S. Federal Bureau of Investigation and CISA released a joint statement to commercial satellite communications providers urging companies to reinforce the cybersecurity and resilience of their networks.

Following the successful cyberattack on Viasat, the Ukrainian government sought help from Elon Musk and SpaceX to help the country restore connectivity through commercial LEO broadband. Only four days after the initial invasion, thousands of Starlink terminals were successfully delivered to Ukraine and reconnected the Ukrainian government and civilians to the internet. Russia attempted to jam SpaceX’s Starlink ground terminals to break Ukrainian communications once again. However, SpaceX was able to quickly counter the attack, and services have not been seriously disrupted since this first attempt in March 2022. According to U.S. Department of Defense leadership, Starlink was able to combat jamming by fixing lines of code, making the Russian attack ineffective. Starlink continues to face attempted jamming by Russian systems, but “their success has been limited.”

Additional jamming has been observed throughout the conflict and in various locations. In March 2022, the European Union Aviation Safety Agency (EASA) released the following:

Spikes indicate unusual GNSS interference in the Eastern Mediterranean. Higher frequency signals have been converted into lower frequency signals to expedite processing.

SPIRE GLOBAL: REPRINTED WITH PERMISSION.
and damaging than its predecessor, the Peresvet. Borisov stated in a TV interview that “if Peresvet blinds an object, the new generation of laser weapons physically destroys the target. It is burned up.” Officials from both the United States and Ukraine commented that these reports have not been substantiated, and there is little evidence to prove that the attack occurred.\textsuperscript{111}

Despite much boasting of capability, there are no independently verified reports of Russia deploying directed-energy capabilities against satellites in its war on Ukraine. Russian officials have showcased the Peresvet in recent years, a ground-based satellite laser. In 2021, President Putin announced that this laser would be adapted for an airborne platform.\textsuperscript{112} Another touted capability is the Sokol-Eshelon, an airborne laser system that is a revival of a Soviet-era program, which has the stated capability to attack satellites in LEO.\textsuperscript{113} Neither of these capabilities have been employed in the Ukrainian conflict despite the high volume of remote sensing satellites and other platforms that are providing data and intelligence on Russian troop positions to the Ukrainian military.

On October 26, 2022, at the United Nations General Assembly, Konstantin Vorontsov, the deputy director of the Russian foreign ministry’s department of nonproliferation and arms, warned that “quasi-civilian infrastructure may become a legitimate target for retaliation.”\textsuperscript{114} This indicates that Moscow considers commercial companies providing services to governments and militaries as legitimate targets in times of conflict.\textsuperscript{115}

\section*{CO-ORBITAL RENDEZVOUS AND PROXIMITY OPERATIONS}

Finally, the Russian inspector satellite Luch may also be supporting Russia’s war on Ukraine through signals intelligence gathering in GEO. At the beginning of 2020, Luch made a significant maneuver westward, covering about 60 degrees in longitude. As it moved, Luch had the opportunity to
RUSSIA

conduct multiple close approaches with other satellites. However, a year later, in March 2021—just months after Russia began its initial military buildup near the Ukrainian border—Luch made a significant maneuver back eastward to visit another Russian satellite in GEO, Cosmos 2520, and an Azerbaijani satellite, Azerspace-2/Intelsat 38. Luch then maneuvered and loitered near Intelsat 33e from October 2021 through January 2022.

As corroborated by data and analysis from commercial space domain awareness company Slingshot Aerospace, Luch moved to rendezvous with Intelsat 39, a high-throughput communications satellite with European coverage, one month before Russia invaded Ukraine. Since the war began, Luch has been performing proximity operations near Intelsat satellites and loitering nearby for about 150 days at each satellite—a significant departure from Luch’s nominal operations since typical loiter times are much less. Notably, these Intelsat satellites are transmitting Ku- and C-band frequencies (which are often used for secure military communications) over Ukraine, although it is unclear if they are supporting any military operations in the region.

Figure 2 Luch Transit before and during Russia’s Invasion of Ukraine

SATELLITE DASHBOARD, HTTPS://SATELLITEDASHBOARD.ORG/.
SLINGSHOT AEROSPACE, HTTPS://SLINGSHOTAEROSPACE.COM/.
India catapulted onto the global counterspace stage in 2019 when it launched its first (and only) ASAT test, becoming only the fourth country to successfully demonstrate a direct-ascent ASAT capability. The Indian space sector continued to grow throughout 2022, with a particular focus on military and private satellite imagery. In October 2022, Prime Minister Narendra Modi announced a new Mission Defense Space Program, where New Delhi highlighted 75 defense space mission areas for private companies to focus on. These 75 missions were separated into five broad categories of space technology for both civilian and military operations: satellite, launch, software, ground systems, and communications and payload.

Space Organization

India’s space program has historically focused on civil and scientific missions, though the past five years have seen expanded military activity. The Indian Space Research Organization (ISRO) is the civilian branch of India’s national space program and has evolved into the sixth-largest space agency in the world. The ISRO operates under the Department of Space, which is headed by the prime minister. Founded in April 2019, the Defence Space Agency (DSA) is charged with upholding India’s national security concerns in space and operates under the Ministry of Defence. The DSA—a collaborative effort between India’s air force, army, and navy—is led by an air force vice marshal and is responsible for the country’s direct-ascent ASAT capability.
Its subsidiary, the Defence Space Research Organisation (DSRO), also established in 2019, absorbed the country’s previous military space agencies, including the Defence Satellite Control Centre and the Defence Imagery Processing and Analysis Centre. The DSRO is led by a senior defense scientist and is responsible for the development of “space warfare systems and associated technology.” There is little documentation on either organization to further describe mandates, goals, or direction.

India’s Defence Research and Development Organisation (DRDO) was founded in 1958 as the primary research and development wing of the Ministry of Defence. The DRDO leads the development of electronic warfare systems, missiles, and radars, among other systems.

SPACE LAUNCH CAPABILITIES

India has three major launch sites in the country: the Vikram Sarabhai Space Centre, the oldest ISRO launch facility in India, which houses the design and development of SLVs; the Satish Dhawan Space Centre, the most popular ISRO launch site due to its geographic superiority; and the Abdul Kalam Island site, which is operated by the DRDO and hosts the Integrated Test Range missile testing facility.

India currently has four active SLVs that are capable of successfully delivering spacecraft to orbit, with at least one new launch vehicle in the testing stage of development. The Polar Satellite Launch Vehicle (PSLV) has been India’s most successful and versatile vehicle, capable of successfully delivering a variety of payloads to orbit. The Geosynchronous Satellite Launch Vehicle (GSLV) focuses on delivering communication satellites to GEO. The Geosynchronous Satellite Launch Vehicle Mark-III (LVM3) is a next-generation versatile vehicle, which can launch communication satellites twice the size of its GSLV predecessor as well as deliver payloads of up to 10 tons to LEO. The ISRO’s first launch in 2023 debuted the agency’s new Small Satellite Launch Vehicle (SSLV-D2), launched from the Satish Dhawan Space Centre. It placed an ISRO Earth observation satellite into orbit along with two private sector satellites—one commercial and one academic. This SSLV-D2 was developed to offer a more available and affordable launch service to the private sector, focusing on small satellite launches.

Two other launch vehicles are in development, the Human Rated Launch Vehicle (HRLV), a follow-on to the LVM3, and the Reusable Launch Vehicle-Technology Demonstrator (RLV-TD). In total, the ISRO has launched 381 foreign satellites from 1999 to 2022.

The country had four successful launches and one failure in 2022: three PSLV launches that placed 15 satellites into orbit, one GSLV launch that delivered 36 OneWeb satellites into orbit, and one failure of the SSLV launcher. Additionally, India has successfully launched two missions to the Moon. Chandrayaan-1 was an orbiter launched in 2008 with a mission life of two years. A decade later, Chandrayaan-2 was launched, a complex mission that consisted of an orbiter, lander, and rover to further explore the south pole of the Moon. The orbiter was able to maneuver to successfully reach its intended orbit and has an estimated mission life of seven years.

The country has a small number of satellites that have been used for military purposes. A large portion of the country’s Geosynchronous Satellite (GSAT) communications constellation is used for military communications. GSAT-7 was the first ISRO satellite to provide services to the Indian military, largely to the Indian navy to enable communications between air, land, submarine,
and warship systems. Similarly, GSAT-7A provides communication services to the Indian air force and army. The country’s first electronic intelligence satellite, EMISAT, is in orbit and is operated by the DRDO. India’s first all-weather radar-imaging satellite, Risat-2, successfully monitored border and maritime activity for the government and re-entered Earth’s atmosphere in 2022 after a 13-year mission. One of India’s most notable satellites, Microsat-R, was operated by the DRDO as an imaging satellite and used as a target for the 2019 destructive ASAT test. Additional reports indicate that India has been investing in the development of military intelligence satellites, specifically focusing on the contested China-India border.

COUNTERSPACE ASSESSMENT OVERVIEW

India’s rise in the space domain is largely due to its demonstrated kinetic direct-ascent ASAT capability launched in 2019. Soon after the test, DRDO officials did not announce specific plans for another ASAT test in LEO but did indicate a possibility of testing in a higher orbit. The possibility of another ASAT test can be seen in research debates across the country. Despite continuing to invest in government and private industry capabilities, there were few public reports of counterspace developments in 2022. The DRDO has sectors focused on the development and design of “electronic, electro-optical and laser based sensors and systems,” though there are no public reports that non-kinetic counterspace capabilities have been developed. It does not appear that India targets space systems in its electronic or cyber systems. India continues to place an emphasis on encouraging developments in the commercial sector to increase its share of the global space economy, boost its domestic technology and industrial sectors, and increase its international standing.
IN 2008, IRAN BECAME THE NINTH COUNTRY TO SUCCESSFULLY place a satellite into orbit using indigenous technologies. Since then, Iran’s space program has become one of the largest in the Middle East, and the country’s leaders regularly invoke the program as a symbol of national strength and progress. However, other countries insist that Iran’s civil and military space programs are cover for Tehran to circumvent international sanctions and develop an offensive ballistic missile and nuclear program. Iran publicly denies any interest in pursuing a nuclear ballistic missile program, claiming its right to pursue a peaceful space program under state sovereignty.

SPACE ORGANIZATION

Iran’s space sector primarily falls under two primary organizations, the civilian Iranian Space Agency (ISA), founded in 2003, and the military Islamic Revolutionary Guard Corps (IRGC) Aerospace Force. While the two are technically separate, they share significant overlap in terms of authority and agenda. The ISA falls under the Ministry of Communications and Information Technology and operates with a Supreme Space Council, which sets policy and is chaired by the Iranian president. The Ministry of Defense is also involved in ISA operations, as its subsidiary groups develop the majority of SLV components and build the satellites. The IRGC is not subject to the policy of the Supreme Space Council and has traditionally focused on developing solid-fuel rockets—not typically used for modern SLVs but well suited for missiles—which
has only increased suspicions about the intent of the IRGC’s space program. Due to international sanctions against supplying ballistic missile technology to the Iranian government, Iran’s private sector has been used as a front to circumvent sanctions and acquire space launch technology. These companies, like the Iranian government, often lack transparency and accountability, and many could likely be considered state-owned enterprises rather than independent businesses contracted by the government.

The early months of 2023 have also seen an uptick of discussion about space in Tehran, with the announcement of a 10-year strategic plan for space released by the ISA in collaboration with the Secretariat of the Supreme Space Council. This document outlines a future where Iran is a regional leader in space technologies and space launch services by 2033. The plan has been applauded by the Iranian president, who added a goal for Iranian-built satellites to orbit in GEO and for independent broadcasting capabilities to be secured. This continues previously stated goals for the burgeoning space program, which included routinely launching satellites into LEO, attaining access to GEO by 2026, and sending an Iranian astronaut to space aboard an Iranian SLV by 2032.

SPACE LAUNCH CAPABILITIES

In 2022, Iran launched two satellites into orbit and had multiple successful tests of new SLVs. This brings the total of Iranian SLVs to five, to include the Safir, Simorgh, Qased, Zuljanah, and Ghaem. Of the five, three are operated by the ISA and two by the IRGC.

The ISA operates the Safir, Simorgh, and Zuljanah. On February 9, 2009, the Safir became Iran’s first SLV to place objects into LEO, featuring a launch range of 300 to 350 kilometers. This success was followed by the Simorgh, with an extended launch range of up to 500 kilometers. After several failed attempts, the Simorgh was successful at placing objects in orbit in 2021. Among other similarities, both SLVs use liquid-fueled engines from the Shahab-3 medium-range ballistic missile. The Zuljanah, which has a hybrid design incorporating solid- and liquid-fuel stages and aims to deliver payloads of 220 kilogram to a 500 km orbit, was successfully tested for a second time in the summer of 2022. However, Iranian SLV progress also saw setbacks, such as the reported explosion of an unspecified SLV on a launchpad in March 2022.

The Qased rocket was the first SLV operated solely by the IRGC and had a successful maiden flight in 2020 to launch Iran’s first military satellite, Noor-1. It was subsequently used to launch the Noor-2 in March 2022. In November 2022, the IRGC also tested a new three-stage solid-fuel launch vehicle, the Ghaem 100, which is designed to reach orbits of 500 kilometers and borrows heavily from the Qased. The Ghaem 100 vehicle is contracted to launch Nahid communication satellites into LEO, potentially in the first six months of 2023. Iran’s SLV and ballistic missile technology is heavily influenced by or acquired from other nations, particularly Russia and North Korea.

Additionally, in October 2022, a third-stage capability, called Saman-1, was tested, which would allow a satellite to change orbits more quickly. This was tested by the Space Research Center and launched by Iran’s defense ministry, with additional interest from the ISA, which indicates that the technology is likely to be used by both the IRGC and the ISA when fully developed.

Iran operates two primary launch sites: the Shahrud Missile Test Site and the Imam Khomeini Space Center. The Shahrud Missile Test Site is located over 400 kilometers east of Tehran and is the predominant launch site of the ISA. The site was built in the 1980s with both Chinese and North Korean assistance. Construction of the Imam Khomeini Space Center, 50 kilometers southeast of Semnan, was completed in 2008 and inaugurated with the launch of a Shahab rocket. Following a destructive rocket launch failure in 2012 and significant construction, the center reopened its doors on July 27, 2017, with the successful launch of a Simorgh SLV.

Additionally, Iran continues to launch satellites from the Russian-leased Baikonur Cosmodrome in Kazakhstan. In August 2022, a Russian rocket launched a remote-sensing Khayyam satellite, which, according to Iran’s information and communications technology minister, Issa Zarepour, was the beginning “of a strategic cooperation between Iran and Russia in the space industry.” The ISA claims that the satellite will send encrypted data to Iranian operators and that Russia will not have access to its data.

SATELLITE CAPABILITIES

Iran currently has three satellites in orbit: the country’s first military satellite, Noor, launched in 2020; Noor-2, a military reconnaissance satellite launched into LEO in March 2022; and the Khayyam Earth-imaging satellite, built and launched by Russia in August 2022. Both Noor satellites collect ISR data, and Iranian officials have released color photographs that the Noor-2 satellite took of U.S. military bases in Bahrain.
In January 2023, the ISA head announced a new telecommunication satellite system, named after former IRGC commander Qassem Soleimani, which is cited as a fundamental element of the 10-year plan for space. Additionally, an Iranian state-run news agency has reported that Iran is capable of building indigenous remote-sensing satellites able to capture images with a resolution of 5 to 10 meters. This capability has not been verified.

Iran is developing other space capabilities as well and is strengthening relationships with other space-faring nations, particularly Russia. The Russian invasion of Ukraine in February 2022 solidified a military alliance between Iran and Russia, and there are reports that Iran is now Russia’s top military supplier. In exchange for Iran’s support, particularly through the supply of UAVs, Russia is likely returning the favor with military and technical support to Iran. Further, in December 2022, the ISA and Roscosmos signed an agreement to design and build remote sensing and communication satellites, develop infrastructure, and hold joint training, which may bolster Iran’s space capabilities in the future.

COUNTERSPACE ASSESSMENT OVERVIEW

After a series of launch failures in recent years, Iran showed signs of progress in 2022. Though Tehran’s launch and satellite capabilities are nowhere near robust, there seems to have been a significant shift in mission success and overall government support of space capabilities. However, Iran appears far from developing kinetic ASAT weapons or non-kinetic physical counterspace weapons. The country continues to develop electronic and cyber capabilities, where Iran has shown success in jamming and hacking against foreign government and commercial satellite communications and the GPS network for years. During periods of civil unrest in the country in 2022, the Iranian government blocked access in Iran to a wide variety of cellular and internet networks, including SpaceX’s Starlink website homepage. Most notably in the last year, French satellite operator Eutelsat revealed details of signals jamming originating in Iran on two of its satellites in the fall of 2022, affecting Persian TV and radio transmissions. The operator notified relevant authorities in Iran.
NORTH KOREA

North Korea’s space capabilities are shrouded in uncertainty. It has been just over a decade since the first successful launch of a North Korean satellite in December 2012, and the country’s space program has since experienced only limited progress. However, 2022 saw an uptick in space activity, including two potential technology tests of components for a future national reconnaissance satellite and upgrades to a space launch facility.

SPACE ORGANIZATION

North Korea’s space activities are centralized under the National Aerospace Development Administration (NADA), which has the stated mission of space development for peaceful purposes, though these claims are often refuted. NADA’s acronym and the organization’s logo resemble the U.S. civil space organization, NASA. NADA was established after the 2013 meeting of the Central Committee of the Workers’ Party of Korea, which adopted a law on space development. This law was revised at a 2022 meeting of the Standing Committee of the 14th Supreme People’s Assembly. State media described the revision as creating basic principles and norms “to ensure space development activities legally and more firmly (sic).” Further details have not been released.
SPACE LAUNCH CAPABILITIES

In 2022, North Korea tested more missiles than any year previously. The country launched over 90 missiles in 2022, including 23 on a single day, November 2, 2022, some within 60 kilometers of the coast of South Korea. Historically, the country’s missile activity has not translated to success for its space program. North Korea reported a space launch test on February 26, 2022, for a spy satellite, a statement the U.S. Department of Defense has refuted as a disguise for an intercontinental ballistic missile system. However, the claim remains consistent with a confirmed “test-piece satellite” launched in December 2022 at the Sohae Satellite Launching Station. Supreme Leader Kim Jong-un visited the Sohae Satellite Launching Station in March 2022 to inspect the spaceport and NADA’s upcoming projects, as well as oversee plans for significant upgrades to the launch site. In December 2022, a new horizontal engine test stand was built and used to conduct its first test, with Kim Jong-un in attendance. North Korea’s second launch site, the Tonghae Satellite Launching Ground, has seen routine maintenance in the last decade but is possibly inactive.

North Korea’s most consistent SLV is the Unha, which has four variants and borrows engine designs from the country’s Nodong medium-range ballistic missile.

SATELLITE CAPABILITIES

North Korea has successfully launched only two Earth observation satellites into orbit, the first in 2012 and another in 2016. After years of failed tests and launches, NADA completed a successful on-orbit “final-stage test” of a military reconnaissance test satellite on December 18, 2022. Ahead of North Korea’s planned first launch of an operational military reconnaissance satellite in April 2023, this technology demonstrator satellite proved camera operability, communication transmission capabilities, and the accuracy of tracking from a ground control system. The test satellite reportedly reached a 500 km orbit with a camera that captured images at 20 m resolution as well as video. Black and white images of Seoul were released by North Korea’s official newspaper, Rodong Sinmun, that were reportedly taken by the test satellite. While not an exquisite system, this rudimentary system would improve North Korea’s limited space capabilities.
NORTH KOREA HAS DEMONSTRATED SMALL SUCCESSES IN ITS SPACE PROGRAM OVER THE PAST YEAR . . . BUT THIS HAS BEEN OVERSHADOWED BY THE IMMENSE NUMBER OF MISSILE LAUNCHES CONDUCTED IN 2022.

NORTH KOREA

COUNTERSPACE ASSESSMENT OVERVIEW

North Korea has demonstrated small successes in its space program over the past year, most notably receiving imagery from a test reconnaissance satellite, but this has been overshadowed by the immense number of missile launches conducted in 2022. While a robust missile launching capability may benefit Pyongyang’s space launch programs, North Korea has yet to exhibit the necessary sensing and altitude control capabilities for a direct-ascent ASAT weapon. It also remains unlikely that North Korea is actively pursuing any non-kinetic physical capabilities. The country has, however, demonstrated successful electronic warfare through GPS and other jamming. North Korea’s cyberattack threat is active and viable, though it is most often used for economic or political messaging rather than aimed at space assets. As the country acquires more advanced technologies, likely through illicit means, and gains operating experience, threats to space systems and ground stations may grow more credible.¹⁹⁵
While the previous chapters have been dedicated to analyzing the countries making the largest strides in counterrspace capabilities, they are not the only ones thinking strategically about the changing space environment. This chapter includes discussion and developments related to counterrspace capabilities by other countries and non-state actors.

Australia

The Defence Space Command of the Royal Australian Air Force was formally established on January 18, 2022, bringing the space elements across the Australian military services into one integrated headquarters organization (similar to the U.S. Space Force). Shortly after, the Australian government released a Defence Space Strategy to build upon the 2020 Defence Strategic Update, declaring the mission is “to prepare space power to secure Australia’s interests in peace and war.” Additionally, the Space Surveillance Telescope (SST), built by the United States and jointly operated with Australia, became operational in September 2022. The SST will provide more accurate space domain awareness by providing tracking and detection of even “faint objects in deep space.” These space domain awareness capabilities are critical to observing and clarifying many space and counterrspace activities outlined in this report, including space launch, RPOs, and ASAT missions.
FRANCE

French officials have continued to be outspoken about investing in counterspace technologies. To spur greater space advancements, Prime Minister Élisabeth Borne announced in September 2022 that the country would be injecting €9.0 billion ($9.6 billion) into the space sector in the next three years. This includes at least €1.5 billion ($1.6 billion) to the country’s civil space agency, the National Centre for Space Studies (CNES). In the same speech, Prime Minister Borne reiterated France’s military space ambitions, largely concentrated on maintaining strategic autonomy in the space domain, including the development of active defenses for space objects. In February 2022, France held its annual space wargame, AsterX, to put elements of the French space defense strategy into practice. Participants from nearly 30 countries were in attendance, spanning military and industry partners. The growth of AsterX emphasizes France’s ambitions as a leader in the military space domain and its intention to grow its defensive counterspace capabilities. After initially publicly discussing the idea of bodyguard satellites in 2019, France is well underway to achieving this capability to protect assets in GEO with a satellite named YODA. Publicly available information states that YODA will have an ISR capability to detect incoming threats to GEO satellites. The first contract for YODA was awarded to Hemeria, a French space start-up.

ISRAEL

As reported in previous years, Israel continues to make progress in testing its Iron Beam capability, a directed-energy system that will complement the Iron Dome missile defense system. This electronic warfare weapon is currently being designed for UAVs and missiles, but with technological changes such as increased power and targeting, it could evolve into a counterspace capability. However, there are no current reports of Israeli leadership steering technology development for Iron Beam in that direction. In April 2022, defense contractor Rafael relayed that the project received renewed funding from the Israeli Defense Forces after successful live-fire tests. Israeli representatives indicated that the Iron Beam could be operational in as few as two to three years. This will be a permanent ground-based system capable of destroying or disabling targets several kilometers away.

JAPAN

In December 2022, Japan released a new national security strategy, national defense strategy, and national defense buildup program, which all emphasize the importance of capabilities in the space domain. These documents add policy positions to an approved 2022 defense budget which dedicated ¥79 billion ($588 million) to capabilities in the space domain, excluding funds tied to ballistic missile defenses. Enhancement of space situational awareness (SSA) capabilities is high on the defense spending list, including development of an on-orbit optical telescope capability, the “procurement of SSA laser ranging equipment” to monitor objects in LEO, interoperability with domestic organizations and the U.S. military, and enhanced satellite communications systems. The 2022 budget document also outlines a reorganization of the Space Operations Squadron, to be broken up into a first squadron to focus on SSA monitoring, a second squadron to focus on the detection of jamming against Japanese satellites, and a third squadron designated as a Space System Management Squadron to manage and maintain space equipment. In January 2023, Japan launched another satellite for its Intelligence Gathering Satellite (IGS) constellation. The IGS-Radar 7 launched from Japan’s Tanegashima Space Center, located on the island of Tanegashima about 40 kilometers south of Kyushu. IGS-Radar satellites are operated by the Cabinet Satellite Information Center, and data is utilized both for national security purposes and civil natural disaster monitoring. This followed a disappointing launch year for the country, in which its only orbital launch attempt in October 2022 failed to reach orbit.

SOUTH KOREA

South Korea’s space program reached a major milestone in June 2022 when the country had its first successful satellite launch using an indigenous liquid-fueled rocket called Nuri. Nuri launched four small satellites to be used for several missions, including Earth observa-
tion. This makes South Korea only the tenth nation to successfully build and launch a rocket. In late 2022, the country’s defense ministry tested a solid-fueled rocket as part of efforts to bolster its defense posture and to launch space-based reconnaissance satellites. Officials, including the newly elected president and science minister, have spoken about commitments to increase the country’s space capabilities, including establishing a state aerospace agency in the future.

UNITED KINGDOM

Following the 2021 establishment of UK Space Command, the United Kingdom’s Ministry of Defence released a Defence Space Strategy in February 2022 focused on operationalizing the space domain. This document serves as a follow-on to the 2021 National Space Strategy and outlines an increase in investment for the UK space sector, injecting an additional £1.4 billion ($1.7 billion) into space systems. This is in addition to £5.0 billion ($6.0 billion) committed to a next-generation military satellite communications constellation.

NON-STATE ACTORS

On March 1, 2022, unconfirmed reports surfaced that non-state actors affiliated with Anonymous—a decentralized international activist and “hacktivist” collective—hacked their way into Roscosmos’ satellite control center. This instance was one of many “hacktivist” activities against Russia after Moscow’s invasion of Ukraine. Dmitry Rogozin, head of Roscosmos at the time, announced that all Roscosmos control centers were operational and that these claims were false. Another hacktivist targeted the Russian Space Research Institute website, leaving crude comments on webpages and threatening further action if Russia did not leave Ukraine. This hacktivist also claimed to be part of Anonymous.
Another year has passed where predictions from previous Space Threat Assessments have been realized. The 2022 report predicted the trend in electronic warfare that “the denial of GPS or satellite communications can have a great effect.”219 This year, while electronic warfare weapons were used on the battlefield in Ukraine, employed early and throughout the war by Russia, the “great effects” that may have been envisioned prior have not been realized. Notably, jamming of GPS and satellite communications did not directly trigger an escalation of the conflict. Past iterations of the report also detailed extensive Chinese counterspace developments. Despite the U.S. Department of Defense characterizing China as the “pacing threat,” Beijing was relatively quiet on the counterspace front this year. This could be for a variety of reasons, but China’s lack of visible activity should not be construed as a decrease in the threat assessment.

The 2022 edition noted a growing number of countries expanding their focus on military operations in the space domain, reorganizing their national security space enterprises, and discussing how to defend space assets, including in cooperation with allies and partners. This trend continues, with examples such as Australia establishing a Defence Space Command in January 2022 and Japan and the United States affirming that attacks “to, from or within space present a clear challenge to the security of the Alliance” and “could lead to the invocation of Article V of the Japan-U.S. Security Treaty.”220
and electronic intelligence capabilities. Coupling its growth in space-based ISR with advancements in artificial intelligence, machine learning, and automation, Beijing is developing, across multiple modalities, an ability to rapidly detect targets and relay those target coordinates to its precision weapon systems to close its own kill chains. The authors anticipate greater public discussions, especially by U.S. national security space leaders, on the policy, capability investments, and operational concepts needed to deny others the use of space against U.S. forces and interests (i.e., U.S. counterspace weapons).

**LESSONS FROM RUSSIA’S INVASION OF UKRAINE**

Previous iterations of this report highlighted Russia’s advanced jamming, dazzling, and cyber capabilities. However, few of these more advanced non-kinetic weapons have been seen in Ukraine, despite social media videos and tweets purporting to show such systems in operation, such as the Krasukha-4 electronic warfare counterspace weapon. Nevertheless, many experts have been surprised at Russia’s lack of success with its electronic warfare systems.

Also absent from the war are laser systems, such as the Peresvet and Sokol-Eshelon, and SAR jamming systems to counter ISR satellites despite the heavy and public use of imagery satellites to track Russian forces. There are several reasons why Russia has not employed such counterspace systems, to the extent such employment would be covered in open-source reporting. It may be that if any attacks were occurring, commercial space companies and Western governments may not want the success of such attacks publicly disclosed. This could be to avoid giving Russia a battle damage assessment and encouragement to use such counterspace weapons against other targets, or to avoid rattling other customers or investors and eroding any competitive advantages. Another possibility is that these Russian systems are not as effective as Western researchers predicted pre-invasion, whether because
the attacks are not as damaging as assumed or that companies, as with SpaceX, have found effective work-arounds to continue operations. It is possible that these systems are inoperable or not as widely deployed as previously assumed. Finally, it could also be that these systems are held in reserve, perhaps viewed as more escalatory or to be used for more strategic purposes. Such use and non-use of different counterspace weapons in Ukraine may be instructive as analysts seek to better understand Moscow’s space strategy and doctrine.

As discussed throughout this report, commercial data and communications services have been integral to Ukraine’s resistance. The former chairman of the State Space Agency of Ukraine, Volodymyr Usov, stated at a December 2022 conference that almost 50 percent of intelligence supplied to Ukraine came from the commercial space industry. Starlink has been called a “lifeline” for Ukrainian forces and civilians alike. Therefore, it is not surprising that Russia targeted and attacked commercial space systems—first Viasat and then SpaceX’s Starlink. As the commercial space sector continues to show its utility in peacetime and conflict for governments and their militaries, the United States’ role in protecting commercial capabilities and strategies for how to do so will be key policy issues for the U.S. government. For starters, commercial operators will increasingly seek threat information from the government that would allow them to make informed decisions on how to better protect constellations or prepare procedures to respond to attacks.

Ukraine’s resistance against Russia is nothing short of remarkable. As researchers who specifically focus on contributions from the space domain to Ukraine’s resistance, the authors ponder how space capabilities can enable David to beat Goliath. Will smaller nations invest in space capabilities to bolster their national security and resilience if attacked, especially by a more powerful nation? Ukraine’s resistance has demonstrated that space capabilities can create an advantage over a more capable military power. Should Taiwan pursue proliferated LEO communications and greater use of commercial ISR data? Conversely, the benefit that space capabilities provide in modern warfare may also provide the justification for adversaries to increase their counterspace weapons development and deny their opponents access to space during a conflict.

Finally, Starlink’s effectiveness in Ukraine has showcased the advantages of proliferated LEO (pLEO) constellations. As more commercial companies and militaries develop pLEO systems, adversaries will seek to counter them. Constellations with satellites in the hundreds and thousands may necessitate a shift in an adversary’s targeting calculus. Kinetic direct-ascent ASATs or kinetic co-orbital weapons that are designed to attack single satellites are less effective unless employed en masse. Moreover, kinetic attacks run the risk of generating a cascading debris field that would make orbits unusable, including for an adversary’s own constellations. An adversary’s options are likely to shift toward cyberattacks, debris-generating attacks to collapse an entire orbital plane, high-altitude nuclear detonations (HANDs), or attacks on physical infrastructure like ground stations. Indicators for such a shift
could include research to understand the effects of HANDs on satellites, for example, as Chinese scientists are reportedly doing at a PLA research institute. Each of these variants of counterspace weapons has policy, operational, and technical trade-offs, and some would be highly escalatory.

SPACE SITUATIONAL AWARENESS

An indicator not addressed in detail in this report is the need for robust space situational awareness (SSA) to enable counterspace weapons targeting. SSA refers to the ability to identify, characterize, and track space objects, where collecting accurate and actionable data is incredibly challenging. Exquisite SSA data is not only advantageous for on-orbit operations of national and commercial satellites but also to provide accurate targeting for counterspace weapons. In order to attack a satellite on-orbit, an aggressor would need to know its precise location and where it is moving. The aggressor will also want accurate battle damage assessments. For example, if a satellite is targeted through a cyberattack that allows the attacker to disable its controls, SSA will be necessary to determine if the attack was successful by monitoring the satellite and any controlled movements. Although this report tracks counterspace weapons developments, it is important to acknowledge the critical data needed to deploy many of these counterspace weapons against targets. Countries that are investing in SSA are not necessarily also developing counterspace weapons; however, countries that are both investing in SSA capabilities and developing counterspace weapons should be watched carefully.

DIRECT-ASCENT ASAT TEST BAN

On April 18, 2022, U.S. vice president Kamala Harris announced a U.S. commitment to stopping destructive direct-ascent ASAT missile testing, an important step forward for sustainability and stability in space. Since then, nine other countries have committed not to conduct destructive direct-ascent ASAT tests, including Australia, Canada, France, Germany, Japan, New Zealand, South Korea, Switzerland, and the United Kingdom. Furthermore, a resolution in the United Nations was adopted on December 7, 2022, that “calls upon all States to commit not to conduct destructive direct-ascent anti-satellite missile tests.” This resolution was passed, with 155 countries voting in support, 9 voting against, and 9 abstaining. Notably, China, Russia, Iran, North Korea, and India did not vote in favor of the resolution. This response to the United States’ unilateral commitment may indicate greater international motivation to develop sustainable norms, behaviors, and agreements to limit the use or testing of counterspace weapons, especially those that create long-lasting orbital debris.
THE PAST YEAR OFFERED A TANGIBLE REMINDER of how important and integral space capabilities have become to citizens across the globe, not only in peacetime but through crisis and conflict. In Ukraine, space capabilities offered: (1) transparency on military aggression by showing the world the buildup and movement of Russian forces; (2) connectivity by enabling Ukrainian forces to transmit information across the battlefield; and (3) a lifeline to the outside world by allowing the Ukrainian people to connect with the world and expose the horrors of war.

But the advantages that space capabilities provide make them a target. The past year showed unusual and threatening behaviors from LEO to GEO, demonstrating that no orbital regime is out of reach of counterspace weapons. It also showed how counterspace weapons have become part of a broader tool kit and military campaign to disrupt command, control, communications, and intelligence gathering and to degrade the effectiveness of UAVs and precision munitions. As China and Russia put more counterspace weapons into operational units, such integration of counterspace weapons and tactics with broader military plans will only increase.

China’s rapid growth in its space capabilities across the PLA’s Strategic Support Force, state-owned enterprises, and burgeoning commercial sector means that it now has a lot to lose. It has quickly become the number two space power, displacing Russia, whose space program is atrophying. CSIS has previously written that “deterrence succeeds by altering the cost-benefit calculus of a potential aggressor.” Beijing’s calculus now involves a high cost, which may give it pause. Moscow’s does not. Notably, no ASAT tests occurred in the past year. Perhaps this is a result of the greater recognition of the destructive potential of debris-generating activity in space, which can ruin orbits for oneself and all others dependent on space, or perhaps it is a result of international efforts in 2022 on norms of behavior and safety and sustainability in space, or it may just be a matter of time before the technology is tested once again. In 2023, it will be important to monitor if this consequential trend is sustained.
ABOUT THE AUTHORS

**KARI A. BINGEN** is the director of the Aerospace Security Project and a senior fellow in the International Security Program at the Center for Strategic and International Studies (CSIS). She joined CSIS from HawkEye 360, an innovative space technology company creating a new class of radio frequency (RF) data and analytics, where she was the chief strategy officer. Prior to the private sector, Kari served as the deputy undersecretary of defense for intelligence and security, overseeing the defense intelligence and security enterprises, comprising more than 120,000 personnel and an annual budget of over $54 billion. Before that, Kari served as the policy director on the House Armed Services Committee and staff lead for its Strategic Forces Subcommittee, advising members of Congress on defense policy, program, and budget matters. Prior to entering government, Kari specialized in national security space issues, working with U.S. defense and intelligence community clients, first as a space systems analyst at SRA International’s Adroit C4ISR Center, and then as a senior space policy analyst at the Aerospace Corporation. In addition to her work at CSIS, Kari is an adjunct assistant professor at Georgetown University, was a commissioner on the CSIS Technology and Intelligence Task Force, and serves on a number of corporate and nonprofit advisory boards. She graduated from the Massachusetts Institute of Technology with a degree in aeronautics and astronautics.

**KAITLYN JOHNSON** is deputy director and fellow of the Aerospace Security Project at the Center for Strategic and International Studies. Ms. Johnson supports the team’s strategic planning and research agenda. Her research specializes in topics such as space security, military space systems, and commercial and civil space policy. 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. She is also a cohost of the CSIS podcast Tech Unmanned, which features guests with both policy expertise and technical expertise in order to break through the national security jargon and technology hand-waving to get to the core of the technical realities of these emerging capabilities, benefits to development, and the barriers to success. 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.

**MAKENA YOUNG** is an associate fellow 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.
INTRODUCTION


TYPES OF COUNTERSPACE WEAPONS


CHINA


Andrew Jones, “China’s Spaceplane Raises Orbit and National Funding.”

Andrew Jones, “China’s Mystery Spaceplane Releases Object into Orbit.”


RUSSIA


Ibid.


90 Harrison, Space Threat Assessment 2020, 26–27.


Harrison et al., Space Threat Assessment 2021, 15.


**INDIA**


123 Vivek Raghuvanshi, “India to Launch a Defense-Based Space Research Agency.”

124 Ibid.


130 Ibid.


after-successful-mission-indias-first-private-rocket-company-skyroot-aerospace-looks-to-slash-satel-
-lite-costs/articleshow/95782212.cms; and “Skyroot Aerospace Plans to Launch Vikram-1 in One Year,”
Satellites.html.
gov.in/Chandrayaan_1.html.
gov.in/Chandrayaan_2.html.
gov/nmc/spacecraft/display.action?id=2013-044B.
www.esa.int/EMISAT.
141 Anjana Pasricha, “India Looks to Enhance Military Capabilities in Space,” VOA News, June 27,
2021, https://www.voanews.com/a/south-central-asia_india-looks-enhance-military-capabil-
ties-space/6207536.html; and “Two Years after Mission Shakti, India Increasing Its Military Capabilities in Space,”
show/81707328.cms?from=mdr.
Microsat_R.html.
143 Snehesh Alex Philip, “DRDO Rules Out A-SAT Tests in Lower Earth Orbits, but Keeps Options Open in Higher Orbits,”
Observer Research Foundation, January 25, 2023, https://www.orfonline.org/expert-speak/an-a-sat-
test-ban-can-wait/.
146 Meera Rohera, “Indian Space Policy for the Private Sector,” Aerospace Security, CSIS, December 7,

IRAN
morgh/.
jordantimes.com/news/region/iran-announces-new-space-launch-amid-nuclear-talks; David Axe,
forbes.com/sites/davidaixe/2021/02/01/irans-new-space-rocket-could-double-as-a-weapon/?sh=2b-
d5eeec82d40; and Patrickintour, “Iran nuclear talks deadlock risks dangerous vacuum,” The Guard-
lock-risks-dangerous-vacuum.
150 “Views and Analysis of the Islamic Republic of Iran on the Resolution ‘Reducing Space Threats
through Norms, Rules, and Principles of Responsible Behavior’ proposed by United Kingdom of Great
Britain and Northern Ireland in the First Committee of the UN (A/C.1/75/L.45/Rev.1) 11/6/2020,” Per-


Ibid.


“Iran Says It Launched Test ‘Tug’ into Suborbital Space,” Associated Press.


Ibid.


Motamedi, “Russia Launches Iranian Satellite into Space from Kazakhstan Base.”


Harrison et al., Space Threat Assessment 2020, 29–34.


OTHERS


and Armée de l’Air et de l’Espace, Twitter post, February 16, 2022, 10:25 a.m., https://twitter.com/Armee_de_lair/status/1494015174617047042.

201 Harrison et al., Space Threat Assessment 2020, 48–49.


207 Japan Ministry of Defense, Defense Programs and Budget of Japan.

208 Ibid.


WHAT TO WATCH

219 Harrison et al., *Space Threat Assessment 2022*.


221 Harrison et al., *Space Threat Assessment 2022*.


CONCLUSION

