APRIL 2021

A REPORT OF
THE CSIS
AEROSPACE
SECURITY
PROJECT

SPACE THREAT ASSESSMENT 2021

Authors
TODD HARRISON
KAITLYN JOHNSON
JOE MOYE
MAKENA YOUNG

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

ABOUT CSIS

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

ABOUT ASP

The Aerospace Security Project (ASP) at CSIS explores the technological, budgetary, and policy issues related to the air and space domains and innovative operational concepts for air and space forces. Part of the International Security Program at CSIS, the Aerospace Security Project is led by Senior Fellow Todd Harrison. ASP's research focuses on space security, air dominance, long-range strike, and civil and commercial space. Learn more at aerospace.csis.org.

ACKNOWLEDGMENTS

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report. As always, the Aerospace Security Project team would like to thank Jeeah Lee, Phillip Meylan, and Emily Tiemeyer for their contributions to the editing, publication, and design of this report. Additional thanks to Thomas G. Roberts for his substantive contributions to this effort.

CSIS does not take specific policy positions; accordingly, all views expressed above should be understood to be solely those of the authors. These views similarly do not necessarily reflect the official policy or position of the U.S. Marine Corps, the Department of the Navy, the Department of Defense, or the U.S. government.

All information is accurate as of March 12, 2021.

CONTENTS

INTRODUCTION

THE PAST YEAR HAS BEEN ONE OF UNCERTAINTY and unpredictability driven by the Covid-19 pandemic, the ensuing global recession, and political change in the United States. For space security, however, 2020 was largely a year of continuity and predictability. Perhaps the most notable change in the space environment since the last *CSIS Space Threat Assessment* was published is the addition of some 900 SpaceX Starlink satellites to low Earth orbit (LEO), bringing the total constellation size to more than 1,200, as shown in Figure 1. This is the largest satellite constellation in history by a wide margin, and it already makes up roughly a third of all operating satellites in space.[1] SpaceX continues to build out its constellation, with launches of 60 Starlink satellites at a time every few weeks.

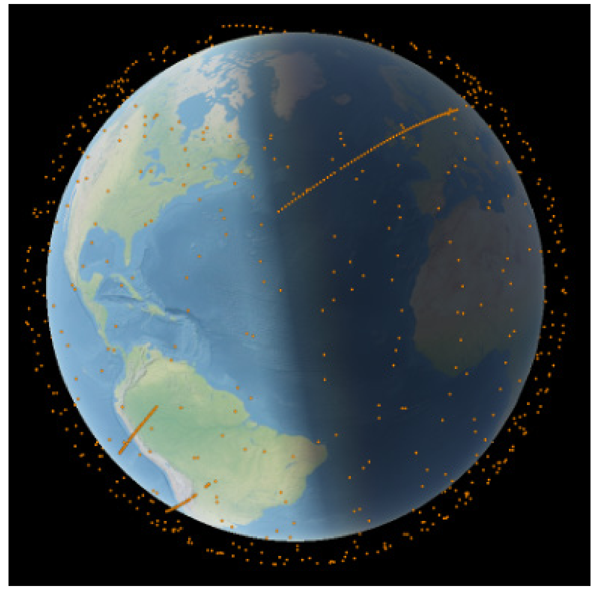


Figure 1 SpaceX's Starlink Constellation as of February 25, 2021

ASTRIAGRAPH

Several notable developments in space policy also occurred in the United States over the past year. Before leaving office, the Trump administration issued three new space policy directives (SPDs). SPD-5 directed government departments and agencies to develop cybersecurity policies and practices to improve the protection of government and commercial space assets from cyberattacks.[2] SPD-6 updated national policy for the development and use of space nuclear power and propulsion, and SPD-7 updated policy and guidance for space-based positioning, navigation, and timing (PNT) programs and activities.[3] The National Aeronautics and Space Administration (NASA) also unveiled the Artemis Accords in 2020, which includes 10 principles nations must agree to abide by to be part of the Artemis program. By the end of the year, eight other countries had signed on to the accords and Brazil issued a statement of intent to sign.[4]

The standup of the U.S. Space Force and U.S. Space Command continued throughout the year as expected. The Space Force submitted its first budget request for $15.4 billion, and $15.3 billion of this was transfers from existing accounts within the Air Force.[5] The Space Force also published its first capstone document, *Spacepower Doctrine for Space Forces*, which was more notable for its continuity with current policy and doctrine than any significant changes.[6] The new commander of U.S. Space Command, U.S. Army General James Dickinson, issued his commander's strategic vision in February 2021, which focused on developing a warfighting mindset throughout the command, maintaining key relationships with allies and partners, and improving integration across the U.S. government and with commercial space organizations.[7]

Throughout the year, other nations continued development and testing of counterspace weapons. Most notably, Russia conducted several antisatellite (ASAT) tests in 2020. As detailed later in this report, Russia tested a co-orbital ASAT weapon in July 2020, and it tested a direct-ascent anti-satellite (ASAT) weapon in December 2020. These activities are not new and reflect a pattern of behavior in which Russia has continued to develop and reconstitute its counterspace capabilities.

The purpose of this annual report from the CSIS Aerospace Security Project is to aggregate and analyze publicly available information on the counterspace capabilities of other nations. It is intended to raise awareness and understanding of the threats, debunk myths and misinformation, and highlight areas in which senior leaders and policymakers should pay more attention. This year's report focuses on the changes in counterspace capabilities and new developments that have occurred or come to light over the past year. A more complete history of counterspace developments can be found on the new CSIS space threat interactive timeline, available at: **https://aerospace.csis.org/counterspace-timeline/**. This online tool will be updated periodically throughout the year and allows users to easily navigate through the large body of publicly available information on space threats, sorting by country, type of threat, and year.

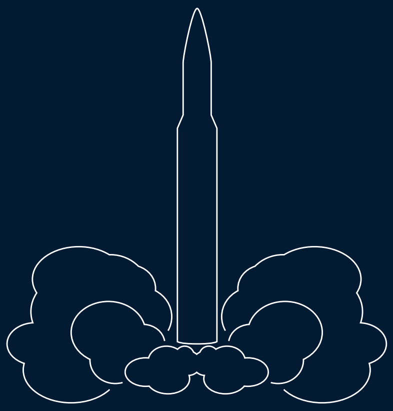
This report and the interactive tool are not a comprehensive assessment of all counterspace activities because much of the information on what other countries are doing is not publicly available. The information in this report is current as of March 12, 2021.

TYPES OF COUNTERSPACE WEAPONS

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."[8]

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 and taxonomy for different types of counterspace weapons. Counterspace weapons vary significantly in the types of effects they create, how they are deployed, how easy they are to detect and attribute, and the level of technology and resources needed to develop and field them. This report categorizes counterpace weapons into four broad groups of capabilities: kinetic physical, non-kinetic physical, electronic, and cyber.

Illustration A ballistic missile can be used as a kinetic physical counterspace weapon.



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 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. Attacks on ground stations are targeted at the terrestrial sites responsible for command and control of satellites or the relay of satellite mission data to users.

Kinetic physical attacks tend to cause irreversible damage to the systems affected and demonstrate a strong show of force that would likely be attributable and publicly visible. A successful kinetic physical attack in space will produce orbital debris, which can indiscriminately affect other satellites in similar orbits. These types of attacks are one of the only counterspace actions that carry the potential for the loss of human life if targeted at crewed ground stations or at satellites in orbits where humans are present, such as the International Space Station (ISS) in 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.

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) that would have indiscriminate effects on satellites in affected orbits. These attacks operate at the speed of light and, in some cases, can be less visible to third-party observers and more difficult to attribute.

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 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

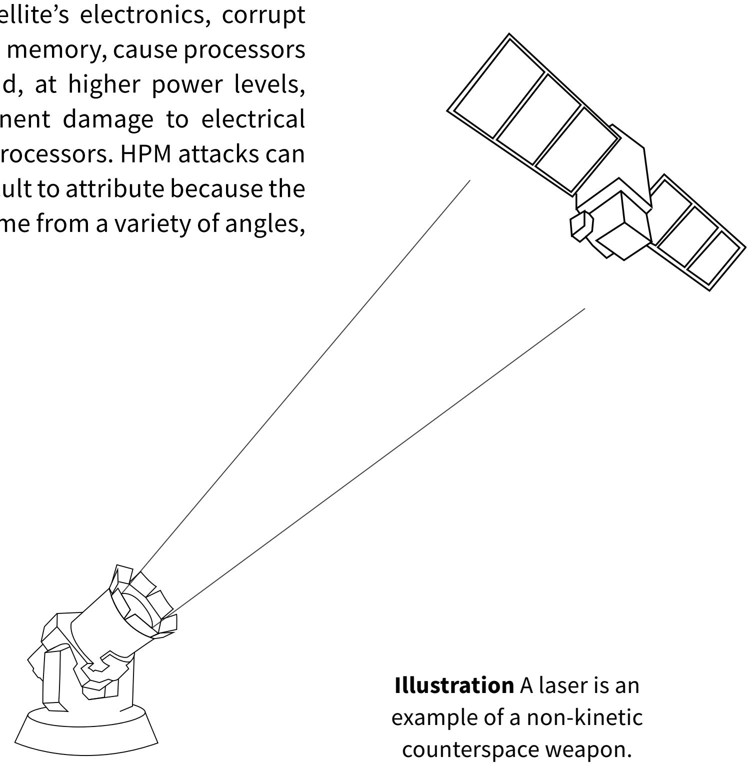


Illustration A laser is an example of a non-kinetic counterspace weapon.

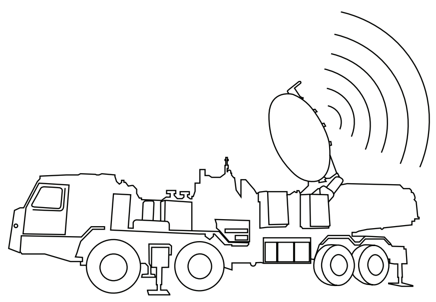


Illustration A truck-mounted jammer is a type of electronic counterspace weapon.

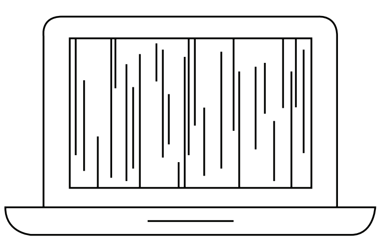


Illustration
Cyberattacks can be used to take control of a satellite and damage or destroy it.

for unshielded satellites in the affected orbital regime. The detonation of nuclear weapons in space is banned under the Partial Test Ban Treaty of 1963, which has more than 100 signatories, although China and North Korea are not included.[9]

ELECTRONIC

ELECTRONIC COUNTERSPACE weapons target the electromagnetic spectrum through which space systems transmit and receive data. Jamming devices interfere with the communications to or from satellites by generating noise in the same radio frequency (RF) band. An uplink jammer interferes with the signal going from Earth to a satellite, such as the command and control uplink. Downlink jammers target the signal from a satellite as it propagates down to users on the Earth. Spoofing is a form of electronic attack where the attacker tricks a receiver into believing a fake signal, produced by the attacker, is the real signal it is trying to receive. A spoofer can be used to inject false information into a data stream or, in extremis, to issue false commands to a satellite to disrupt its operations. User terminals with omnidirectional antennas, such as many GPS receivers and satellite phones, have a wider field of view and thus are susceptible to downlink jamming and spoofing from a wider range of angles on the ground.[10]

Electronic forms of attack can be difficult to detect or distinguish from accidental interference, making attribution and awareness more difficult. Both jamming and spoofing are reversible forms of attack because once they are turned off, communications can return to normal. Through a type of spoofing called "meaconing," even encrypted military GPS signals can be spoofed. Meaconing does not require cracking the GPS encryption because it merely rebroadcasts a time-delayed copy of the original signal without decrypting it or altering the data.[11] 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 in a system. These attacks can target ground stations, end-user equipment, or the satellites themselves. While cyberattacks require a high degree of understanding of the systems being targeted, they do not necessarily require significant resources to conduct. The barrier to entry is relatively low and cyberattacks can be contracted out to private groups or individuals. Even if a state or non-state actor lacks internal cyber capabilities, it may still pose a cyber threat.

A cyberattack on space systems can result in the loss of data or services being provided by a satellite, which could have widespread systemic effects if used against a system such as GPS. Cyberattacks could have permanent effects if, for example, an adversary seizes control of a satellite through its command and control system. An attacker could shut down all communications and permanently damage the satellite by expending its propellant supply or issuing commands that would damage its electronics and sensors. Accurate and timely attribution of a cyberattack can be difficult because attackers can use a variety of methods to conceal their identity, such as using hijacked servers to launch an attack.

Table 1

TYPES OF COUNTERSPACE WEAPONS

	Kinetic Physical			Non-kinetic Physical			
Types of Attack	**Ground Station Attack**	**Direct-Ascent ASAT**	**Co-orbital ASAT**	**High Altitude Nuclear Detonation**	**High-Powered Laser**	**Laser Dazzling or Blinding**	**High-Powered Microwave**
Attribution	Variable attribution, depending on mode of attack	Launch site can be attributed	Can be attributed by tracking previously known oribt	Launch site can be attributed	Limited attribution	Clear attribution of the laser's location at the time of attack	Limited attribution
Reversibility	Irreversible	Irreversible	Irreversible or reversible depending on capabilities	Irreversible	Irreversible	Reversible or irreversible; attacker may or may not be able to control	Reversible or irreversible; attacker may or may not be able to control
Awareness	May or may not be publicly known	Publicly known depending on trajectory	May or may not be publicly known	Publicly known	Only satellite operator will be aware	Only satellite operator will be aware	Only satellite operator will be aware
Attacker Damage Assessment	Near real-time confirmation of success	Near real-time confirmation of success	Near real-time confirmation of success	Near real-time confirmation of success	Limited confirmation of success if satellite begins to drift uncontrolled	No confirmation of success	Limited confirmation of success if satellite begins to drift uncontrolled
Collateral Damage	Station may control multiple satellites; potential for loss of life	Orbital debris could affect other satellites in similar orbits	May or may not produce orbital debris	Higher radiation levels in orbit would persist for months or years	Could leave target satellite disabled and uncontrollable	None	Could leave target satellite disabled and uncontrollable

	Electronic			Cyber		
Types of Attack	**Uplink Jamming**	**Downlink Jamming**	**Spoofing**	**Data Interccept or Monitoring**	**Data Corruption**	**Seizure of Control**
Attribution	Modest attribution depending on mode of attack	Modest attribution depending on mode of attack	Modest attribution depending on mode of attack	Limited or uncertain attribution	Limited or uncertain attribution	Limited or uncertain attribution
Reversibility	Reversible	Reversible	Reversible	Reversible	Reversible	Irreversible or reversible, depending on mode of attack
Awareness	Satellite operator will be aware; may or may not be known to the public	Satellite operator will be aware; may or may not be known to the public	May or may not be known to the public	May or may not be known to the public	Satellite operator will be aware; may or may not be known to the public	Satellite operator will be aware; may or may not be known to the public
Attacker Damage Assessment	No confirmation of success	Limited confirmation of success if monitoring of the local RF environment is possible	Limited confirmation of success if effects are visible	Near real-time confirmation of success	Near real-time confirmation of success	Near real-time confirmation of success
Collateral Damage	Only dirupts the signals targeted and possible adjacent frequencies	Only disrupts the signals targeted and possible adjacent frequencies	Only corrupts the specific RF signals targeted	None	None	Could leave target satellite disabled and uncontrollable

CHINA

MINIMAL COUNTERSPACE WEAPONS DEVELOPMENTS or tests were identified in open-source information over the past year. However, as has been reported in previous iterations of this report, China has a robust direct-ascent ASAT program, dual-use capabilities on orbit that are necessary for co-orbital ASAT weapons, and widely used electronic and cyber counterspace capabilities.[12]

Despite the global pandemic, 2020 saw many accomplishments for China in civil space missions. The Chang'e-5 Moon mission returned 2 kilograms, or about 4.5 pounds, of lunar regolith in December 2020.[13] The *Yutu-2* rover is still operating on the far side of the Moon and has traveled over 600 meters, or over 2,000 feet, on the lunar surface.[14] China also plans to launch the core section of its national space station in 2021.[15]

In June 2020, China launched its first Mars rover, *Tianwen 1*, which entered Martian orbit in February 2021 and will likely land on Mars in May or June 2021. The planned mission is for the rover to operate for 92 Martian days (about 95 days on Earth).[16] China is one of three countries pursuing missions to Mars in 2021, with the United States landing the *Perseverance* rover on February 18, 2021 and an orbiter mission from the United Arab Emirates entering Mars orbit in February 2021.

CHINA

China successfully launched the final positioning, navigation, and timing (PNT) BeiDou satellite of the current constellation in June 2020. Essentially a Chinese version of GPS, the BeiDou constellation is now composed of 35 satellites in orbit that provide location and timing services to over 120 countries.[20] BeiDou has been in the works for over two decades and allows China to be independent of the U.S. GPS system for national PNT.[21] Notably, BeiDou has been a cornerstone of the Chinese Belt and Road Initiative.

China's space launch vehicle (SLV) program suffered a setback in March 2020 when the inaugural launch of the Long March 7A failed due to an engine malfunction and the payload was lost. However, almost exactly one year later, on March 12, 2021, the Long March 7A SLV successfully delivered its first payload into orbit, a classified, experimental satellite. The Long March 7 series is intended to deliver payloads into geostationary (GEO) orbit and to launch cargo to China's upcoming national space station. Long March 8, the next SLV in the Long March family, is currently in development and will boast a recoverable and reusable first stage, much like SpaceX's Falcon family.[22]

SPACE ORGANIZATION

The organization of space assets and missions within China's People's Liberation Army (PLA) remains unclear. Many space missions, such as space launch and the acquisition and operation of satellites, remain within the Strategic Support Force (SSF). Often presented as the "information domain," the SSF maintains PLA efforts for cyber, electronic, and psychological warfare, as well as space. According to experts, the Space Systems Department and Network Systems Department (co-equal semi-independent branches within the SSF) share joint missions, including counterspace capabilities. A Center for the Study of Chinese Military Affairs report notes that, "another important principle that appears to have influenced the design of the SSF is the enduring Maoist imperative of peacetime-wartime integration."[23] This principle is well suited for the dual-use nature of many space and counterspace capabilities.

Chinese civil space capabilities, such as the Martian rover, are led by the China National Space Administration (CNSA), which falls within the purview of the State Council's State Administration for Science, Technology, and Industry for National Defense (SASTIND). The China Aerospace Science and Technology Corporation (CASC) and China Aerospace Science and Industry Corporation (CASIC) are two examples of the many research and development arms of the Chinese government which specialize in space technologies.[24]

China's spaceplane is rumored to be similar to the United States' X-37B (pictured above).

U.S. AIR FORCE

China's New Spaceplane

A NOTABLE DEVELOPMENT IN 2020 was the launch and recovery of a national spaceplane, similar to the United States' X-37B spaceplane program. The Chinese space plane was launched by a Long-March 2F on September 4, 2020, and after orbiting Earth in LEO for two days, it successfully landed in northwest China on a five-kilometer runway. The United States has catalogued at least two new objects in orbit that were likely deployed by the space plane.[17] Experts, however, are uncertain of the motivations behind or mission of this new space plane, but it is unlikely to be used as a counterspace weapon.[18] Unrelated to this space plane test is the Tengyun project, a horizontal takeoff and landing spacecraft to be completed by 2025. Not many details have been released publicly about the success of this program, which is intended to provide a rapid launch capability.[19]

COUNTERSPACE WEAPONS

Kinetic Physical

China continues to conduct tests of its operational SC-19 direct-ascent ASAT system.[25] However, China no longer needs to use kinetic tests to prove its direct-ascent ASAT capabilities can threaten any U.S. satellite in LEO, and likely medium Earth orbit (MEO) and GEO as well.

The notorious Chinese inspector satellite, dubbed Shijan-17 (SJ-17), was relatively quiet this past year but did make a few stops near other satellites as it moved around the GEO belt. According to CSIS analysis, SJ-17 performed three enduring rendezvous proximity operations (RPOs) nearby other Chinese satellites, Chinasat 6B, SJ-20, and Gaofen 13 (GF 13). After a long period of inactivity that lasted about a year, SJ-17 restarted its unusual movements in late 2019. From December 2019 through late January 2020, SJ-17 was in close proximity to Chinasat 6B, a television broadcasting communications satellite. SJ-17 then drifted slightly eastward to rendezvous with another experimental Chinese satellite, SJ-20, from late January through early April 2020. The closest SJ-17 and SJ-20 were to one another was under five kilometers.[26] After this encounter, SJ-17 performed an unusual drift to station itself about 50 degrees eastward. Three months later, SJ-17 performed a westward drift that allowed it to be in close proximity with GF 13, a Chinese Earth observation satellite.[27]

Tianjin University has developed a new robot intended to support space debris-removal missions. This tentacle-like robotic arm would be placed on satellites and launched into orbit to then grapple debris and clear it from popular orbits. However, the robotic arm could in theory be used to grab an adversary's satellite.[28] Furthermore, the design of the arm would probably require an extremely close RPO that would not be effective with debris or defunct satellites that could be tumbling uncontrolled in space. The target debris would likely need to be in a predictable motion in an established orbit in order for capture by the robotic arms to be possible. The design of this satellite lends itself to a co-orbital ASAT, even if that is not the stated intent.

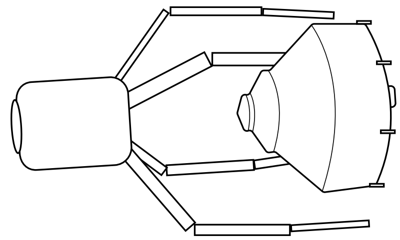


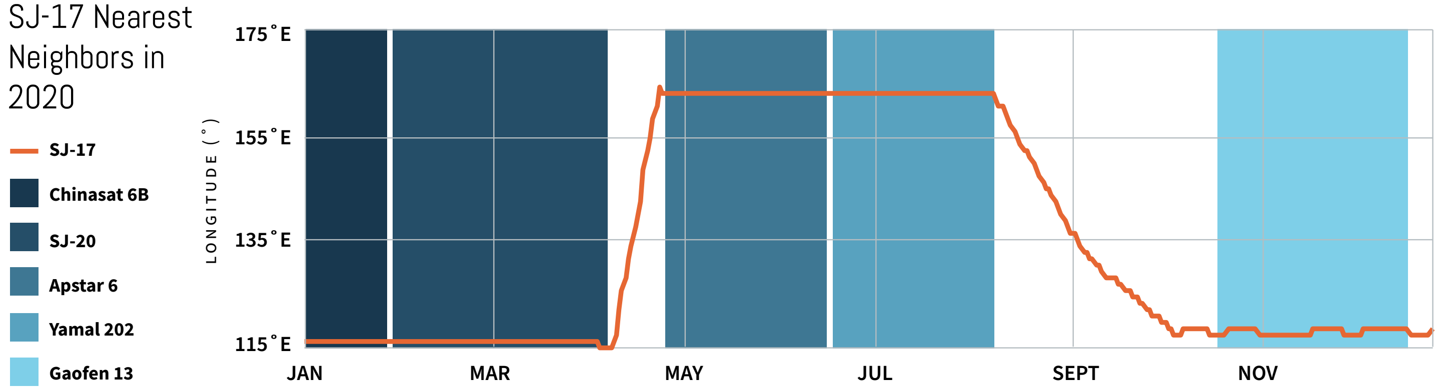
Illustration New robot designed by Tianjin University shown capturing a satellite on orbit.

CHINA . . . CAN THREATEN ANY U.S. SATELLITE IN LEO, AND LIKELY IN MEO AND GEO AS WELL.

Chinese Rendezvous and Proximity Operations in GEO. Publicly available orbital positioning data suggests that Chinese satellite SJ-17 has made several close approaches and inspections in GEO. Learn more about SJ-17's behavior, including a list of the satellite's nearest neighbors. at **aerospace.csis.org/SJ17**.

SPACE-TRACK.ORG / CSIS AEROSPACE SECURITY

SJ-17 Nearest Neighbors in 2020



Map of the Ladakh Region, where Chinese satellite jammers are rumored to be placed 60km from the border.

Non-kinetic Physical

Some analysts have made recent claims of massive developments in Chinese ground-based laser stations, including the identification of five suspected locations of such programs within China. While some of the programs identified appear to be academic and therefore are likely not ASAT systems, one location of primary concern is a military base known for conducting kinetic physical ASAT tests that is also rumored to house a laser weapon system.[29] There is no indication of how advanced or "ready-to-mobilize" such a directed energy system may be, and there has been no publicly available information about potential tests or attacks against space systems.

Electronic

In late October 2020, an Indian news source, the Hindustan Times, accused China of moving mobile jammers within 60 kilometers of the Line of Actual Control (LAC) in Ladakh , part of the disputed Kashmir region between India, Pakistan, and China. The source asserts that the movement of jamming technology into the region is intended to hide PLA movements in the area.[30] Despite efforts from the CSIS study team, these claims could not be substantiated by another source.

Cyber

There have been no recent publicly acknowledged cyberattacks from China against the United States' or other nations' space systems. However, China has successfully proven this capability before and continues to be active with cyberattacks in other domains against financial or defense-related targets.

RUSSIA

THOUGH MOST INDUSTRIES, AND A LARGE PORTION OF OTHER countries mentioned in this report, were slowed down due to the Covid-19 pandemic, Russia's military space capabilities kept a steady pace. In the last year, Russia tested numerous counterspace capabilities, performed complex RPOs, and expanded its space-based military infrastructure. The country's consistent space launch capability, the continuous advance of counterspace capabilities, and civil space contributions through the ISS have maintained Russia's status as a major space power, and its prowess in the space domain has fostered unique relationships with foreign countries that are sometimes rivals in other domains.

SPACE ORGANIZATION

Russia's state-sponsored space activities fall into either the Russian Aerospace Forces (RAF) or the civil Roscosmos program. Within the Russian military, space capabilities fall under the RAF. A subsection of the RAF is the Russian Space Force, which was created in 1992 as the world's first space force and is responsible for the monitoring of all space-based assets, military launches, and potential threats to space systems.[31]

Roscosmos is a longtime partner of NASA, and the two agencies, together with Japan, Canada, and Europe, serve as the principal partners on the ISS. Roscosmos CEO Dmitry Rogozin announced that there were 17 launches of rockets in 2020 and 29 space launches planned for 2021. Rogozin also confirmed the country will begin exploration of the Moon via automated modules and lunar probes, followed by a crewed program.[32] The crewed program is slated to land on the Moon in 2030, with regular missions to follow. Roscosmos has also announced plans for a permanent lunar base to begin in 2035.[33] Additionally, Russia has ongoing discussions with China to establish a Moon research base. Roscosmos and China's space agency signed a 5-year space cooperation program in 2017.[34] In February of 2021, the Roscosmos press office confirmed that the agency was ready to sign an agreement with the "Government of People's Republic of China on cooperation to create the International Lunar Research Station," and the two space agencies signed a memorandum of understanding on March 9, 2021.[35] A statement from Roscosmos outlined a plan of cooperation with international partners "with the goal of strengthening research cooperation and promoting the exploration and use of outer space for peaceful purposes." To further solidify their relationship in space going forward, the two countries signed another agreement to create a data center to assist in future missions to the Moon and deep space.[36]

RUSSIA'S PROWESS IN THE SPACE DOMAIN HAS FOSTERED UNIQUE RELATIONSHIPS WITH FOREIGN COUNTRIES THAT ARE SOMETIMES RIVALS IN OTHER DOMAINS.

To aid in these goals, Russia continued testing a new SLV called the Angara, which is the first SLV fully developed in post-Soviet Russia. The Angara family of vehicles will include both heavy and light launch vehicles, all of which will be capable of reaching LEO and two of which will be capable of reaching GEO.[37] Angara vehicles resumed testing in December of 2020 and are planned to be batch-produced for both Roscosmos and the Russian Ministry of Defence beginning in 2023. Roscosmos also announced plans to begin building satellites for foreign partners, which will include telecommunication and remote sensing satellites.[38]

In 2020, Russian president Vladimir Putin approved a document which empowers him to use nuclear weapons in response to a conventional strike targeting the country's critical government and military infrastructure. In addition to defending against conventional weapons, space-based weapons are mentioned as a threat in the document. The document also calls out the potential deployment of missile defense and offensive strike weapons in space as posing a threat to Russia.[39] The approval of this document signals that Russia believes space-to-Earth weapons could pose as much of a threat as nuclear weapons and would elicit the same response from the country.

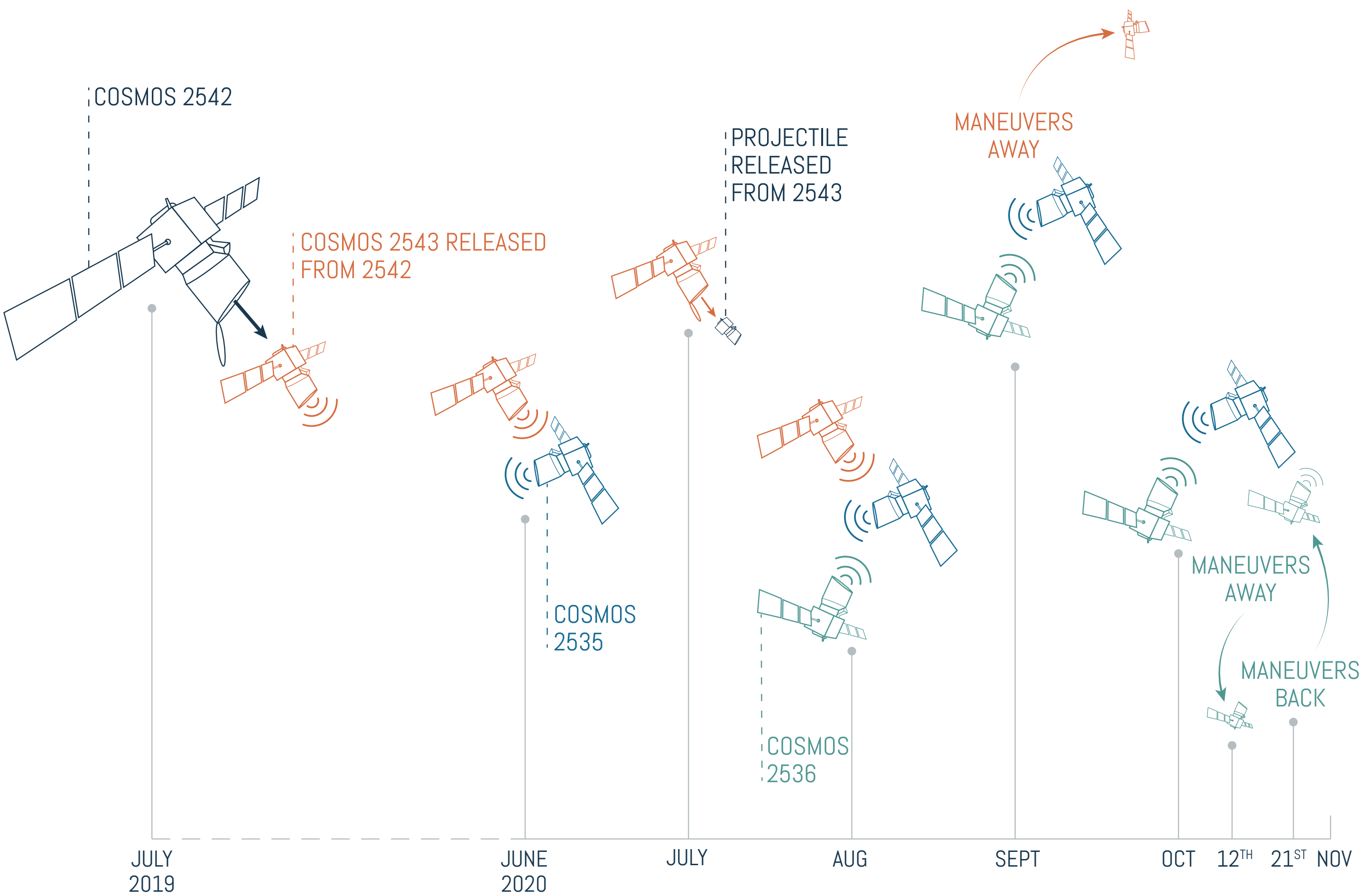
COUNTERSPACE WEAPONS

Kinetic Physical

Russia has possessed kinetic physical counterspace capabilities since the Soviet Union's first co-orbital ASAT test in the 1960s. The technology used in Soviet-era programs proved to be solid building blocks for more recent Russian developments, and the country has repeatedly displayed direct-ascent and co-orbital ASAT capabilities—both of which were tested over the past year.

On April 15, 2020, Russia tested its PL-19/Nudol direct-ascent ASAT system, which was publicly condemned by U.S. Space Command.[40] The PL-19/Nudol was launched from the Plesetsk Cosmodrome in northern Russia, travelling 3,000 kilometers before splashing down in the Arctic Ocean. This test did not appear to make a kinetic impact with anything in LEO.[41] On December 19, 2020, Russia tested the system once again, further prompting U.S. Space Command officials to state that "Russia's persistent testing of these systems demonstrates threats to U.S. and allied space systems are rapidly advancing."[42] These appear to be the ninth and tenth tests of this system, the last eight of which were successful.[43]

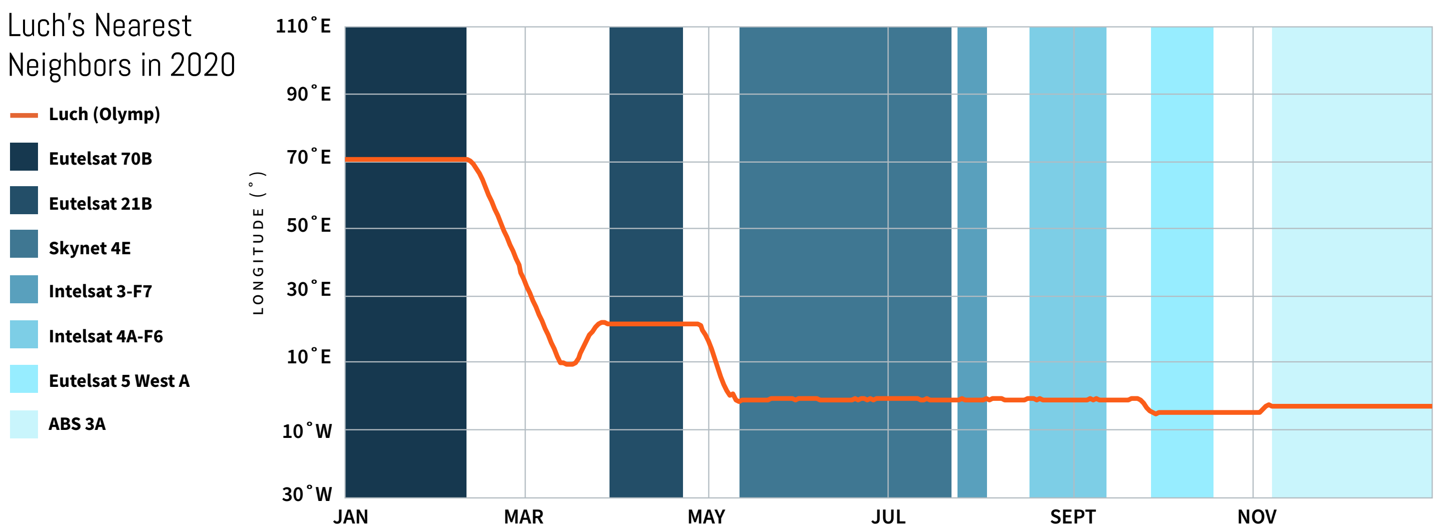
In addition to the repeated testing of the Nudol direct-ascent ASAT capability, the United States accused Russia of conduct-



Russian Co-orbital ASAT Test in LEO, 2019-2020

ing a co-orbital ASAT test in July 2020. This test was more sophisticated than the direct-ascent ASAT test, involving a Russian satellite Cosmos 2542 which contained a smaller satellite inside of it, labeled Cosmos 2543. Cosmos 2542 ejected Cosmos 2543 in 2019. On July 15, 2020, Cosmos 2543 fired a small projectile near an unrelated Russian satellite, Cosmos 2535.[44] This instance mimicked a similar operation with nesting satellites in 2017 when satellite Cosmos 2521 was ejected from its mother satellite Cosmos 2519.[45] In response to the July 2020 test, U.S. Space Command released a statement which condemned this test and asserted that the small projectile fired from Cosmos 2543 could be used to target satellites. In response, the Russian Ministry of Defence said these matryoshka, or nesting, satellites are deployed for routine inspections and surveillance of Russia's other space assets.[46] The Kremlin has continued to assert that Russia has always been and remains a country that is committed to the goal of fully demilitarizing outer space and not deploying weapons in outer space.[47]

Since being ejected from its mother satellite, Cosmos 2543 has been very active. Before firing the projectile in July 2020, the inspector satellite was constantly changing its orbit to synchronize with other Russian satellites. This is out of the ordinary for most satellites, which rarely maneuver in this way. In June of 2020, Cosmos 2543 joined Cosmos 2535 in orbit.[48] For months the two satellites performed RPOs with one another and an additional satellite, Cosmos 2536. In September 2020, Cosmos 2543 began to drift away from the others, but Cosmos 2535 and 2536 continued to remain close to one another for several weeks. The two satellites were so close together that it is possible they performed docking maneuvers; however, it is hard to be certain without increased space domain awareness (SDA). One SDA ground observation reported a single object, instead of two unique objects, which further increased speculation that the satellites docked. On October 12, 2020, Cosmos 2536 and 2535 separated, and four days later Cosmos 2536 was reportedly 20 kilometers from *Cosmos 2535.* By October 21, Cosmos 2536 was again within a kilometer of Cosmos 2535.[49] While not a weapons test, this much movement in orbit is highly unusu-



Luch Continues to Explore the GEO Belt. The Russian satellite has made several close approaches and inspections in GEO since its launch in 2014, including those depicted here in 2020. Learn more about Luch's behavior, including a list of the satellite's nearest neighbors at **aerospace.csis.org/luch**.

SPACE-TRACK.ORG / CSIS AEROSPACE SECURITY

al and raises suspicions about the motivations behind such space capabilities.

In addition to the movements of the Cosmos satellites, the Russian satellite Luch contributed co-orbital activities in 2020. Luch has been consistently moving around in the GEO belt since its 2014 launch and continued to perform RPOs in the past year. According to CSIS analysis, the satellite maneuvered next to seven satellites, which included European, UK, U.S., and Asian broadcast satellite operators. Though these orbital maneuvers are no longer rare for this particular satellite, the vast majority of satellites that operate in GEO are stationary, which makes the activity of Luch highly unusual year after year.

Russia continues to develop its air and missile defense systems. Though not officially designated as ASAT weapons, the S-400 and S-500 series surface-to-air (SAM) missile systems could likely reach a satellite in LEO.[50] The S-500 was heavily tested in 2020 and is scheduled to be completed in 2021 as a replacement for the capable S-400. Russian military sources claim that the missile is designed to strike objects in space as well as defend areas from space-based weapons. The head of Russia's Air and Space Forces has said that the S-500 is capable of destroying hypersonic weapons and satellites in near space.[51] Asserting further that the missile class will be able to be used as a counterspace weapon, the deputy chief of the RAF's SAM troops, Yuri Muravkin, said that "the boundaries between air and space are being and will be erased as the aerial enemy gradually becomes an aerospace one."[52]

A New Update on an Old Weapon

NEW INFORMATION EMERGED IN 2020 about an old Soviet-era space weapon. The Soviet Union's R-23M cannon is known as being the only gun fired in space. The system reached orbit on June 25, 1974, and the cannon was tested on its last day in space in 1975. A reported 20 shells were fired from one to three blasts, which all burned up in the atmosphere. The gun was originally developed to help protect airborne bombers, but its small frame and lightweight made it an easy choice to attach to a spacecraft. A factory visit in early 2021 produced the second known photo of the only cannon to be fired in orbit .[53]

Non-kinetic Physical

As with kinetic counterspace capabilities, Russia continues to maintain a variety of non-kinetic counterspace weapons. Announced by Russian president Vladimir Putin in 2018, the Peresvet laser system was thought to be a mobile trailer-mounted laser system, but plans to put Peresvet on an airborne carrier were made public in 2021.[54] The Peresvet system will be the second airborne laser system in development by Russia, following Sokol-Echelon, which was announced in September 2016 and has been reported as likely to have

Mobile Tirada-2 satellite jamming systems

RUSSIAN MINISTRY OF DEFENSE

ASAT capabilities.[55] Sokol-Echelon's chief designer claimed the laser system was a response to the U.S. withdrawal from the Anti-Ballistic Missile (ABM) Treaty in 2002 and that it was intended to counter "air-based and space-based reconnaissance assets."[56]

Electronic

Russia continues to grow its electronic counterspace capabilities and has recently focused on developing mobile ground-based systems to interfere with foreign satellites.[57] Electronic capabilities have been increasing at a steady pace since the early-2000s and accelerated in 2009 with the standup of Electronic Warfare Troops within the Russian military. Recent developments in electronic counterspace weapons include the Tirada-2 , a mobile jamming system "for suppression of space communications."[58] Another electronic warfare system in development is the Bylina-MM, a ground-based mobile system with a focus on jamming satellite communication channels. Bylina has been reported as "a series of ground-based mobile automated stations" and a mobile command and control system with artificial intelligence (AI).[59] It includes an automated system that is able to recognize assets and determine how to attack them, and it can be used against a variety of ground, air, and space-based targets. Russia also reportedly has two radar jammers, called Krasukha-2 and Krasukha-4, which may be capable of interfering with radar reconnaissance satellites.[60]

The first Russian orbital launch of 2021 included a satellite to be added to the Liana constellation, an electronic intelligence program for space-based surveillance and targeting.[61] The satellites in this constellation are designed to intercept radio communications and can be used to detect objects on the surface the size of a car.[62] Additionally, Russia is developing ground-based signals intelligence (SIGINT) sites under the name Sledopyt with the capability to gain access to radio signals emitted by foreign satellites orbiting above Russian territory.[63] Another project, known as Tobol, or 8282, has been described as "electronic warfare complexes for space-related purposes," and infrastructure related to this system was built near satellite tracking facilities.[64]

Cyber

Russia flexed its offensive cyber capabilities in 2020 in what is being called "one of the most devastating cyberattacks in history."[65] This hack, commonly known as the SolarWinds breach because access was gained through a network management software company of the same name, is reported to have affected over 250 U.S. federal agencies and businesses, to include the U.S. State Department, parts of the Pentagon, and the cybersecurity firm FireEye.[66] Before President Joe Biden took office, he affirmed that the United States must be able to quickly deter and disrupt future cyberattacks and stated that he would "not stand idly by in the face of cyber assaults on our nation."[67] The SolarWinds attack is the latest in a long line of large Russian hacking incidents, similar to the 2017 NotPetya attack. This incident targeted Ukrainian companies such as Antonov, a Ukrainian aircraft manufacturing company, and the Kyiv International Airport in Zhuliany.[68]

IRAN

DESPITE ADVANCEMENTS IN ITS SPACE LAUNCH PROGRAM in the past year, Iran's counterspace capabilities have not shown significant progress. Iran still appears far from developing a viable direct-ascent ASAT weapon; however, many scholars and world leaders continue to accuse Iran of using space launches as a veil for its ballistic missile program.[69] To make significant progress on kinetic and non-kinetic physical counterspace systems, Iran would likely need to acquire technology and resources from a major counterspace actor, such as Russia or China, as reports indicate they have in the past.[70] Iran continues to develop electronic and cyber counterspace capabilities and demonstrates increased success in jamming and hacking attacks against foreign governments and civilian systems.

SPACE ORGANIZATION

Iran's space programs fall under two primary organizations. The Iranian Space Agency, under the oversight of the Ministry of Information and Communication Technology and the direction of the Supreme Space Council, is the civilian entity responsible for policy, research and development, and cooperation for peaceful civilian space issues.[71] Iran's military space program is headed by the Islamic Revolutionary Guard Corps (IRGC) Aerospace Force.[72] The IRGC's redesignated its Air Force to the Aerospace Force in

IRAN'S COUNTERSPACE CAPABILITIES HAVE NOT SHOWN SIGNIFICANT PROGRESS.

2009, indicating Iran's recognition and elevation of space forces and capabilities within the military.[73] As further evidence of this, Iran revealed the existence of its own Space Command in April 2020 after a successful satellite launch by the IRGC.[74] There is no open-source reporting to provide details as to the IRGC Space Command's organization, capabilities, and missions; however, it is reasonable to surmise that this new organization is responsible for all space- and counterspace-related forces and missions within the IRGC.

SPACE LAUNCH CAPABILITIES

After several failed launch attempts by the Iranian Space Agency in 2019 and early 2020, the IRGC successfully launched its first military satellite into LEO on April 22, 2020.[75] Named Noor-1, the satellite is reported to be a 3U or 6U CubeSat, weighing roughly 15 to 30 pounds.[76] Iranian news sources reported that the satellite was successfully placed into a 425-kilometer orbit.[77] IRGC Commander Major General Hossein Salami referred to the satellite as "multi-purpose," highlighting its strategic intelligence-gathering capabilities.[78] An Iranian report added that the Noor-1 satellite is a reconnaissance satellite with visual and thermal monitoring technology.[79] Many experts believe it is a rudimentary satellite with limited capabilities.[80] Shortly after launch, the U.S. Space Force's 18th Space Control Squadron tweeted that it was tracking both the satellite and the rocket's upper stage.[81] This launch has three notable differences from previous Iranian launches.

First, the Qased launch vehicle purportedly is a three-stage system. Its first stage is comprised of a liquid-propellant ballistic missile called Ghadr, which is an upgraded version of the Shahab.[82] What makes this launch vehicle different for Iran is the second and third stages. The second stage used a solid-propellant motor called the Salman, which has sophisticated technologies such as a carbon-fiber motor casing and a swiveling thrust vector control nozzle. Less is known about the third stage; however, some statements indicate that it was a smaller solid-propellant kick motor, often used to help deliver a satellite to its final orbit.[83] The successful incorpora-

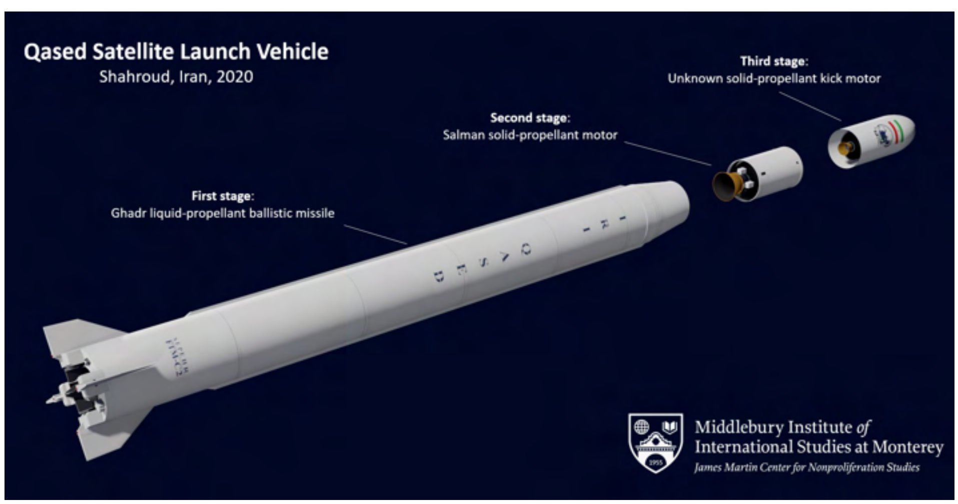


IMAGE COURTESY OF THE JAMES MARTIN CENTER FOR NONPROLIFERATION STUDIES AT THE MIDDLEBURY INSTITUTE OF INTERNATIONAL STUDIES IN MONTEREY, CALIFORNIA tion of solid-fuel motors is a technological advancement not previously reported in Iranian SLV capabilities.

Second, the launch was conducted by the IRGC, as opposed to the Iranian Space Agency, which was responsible for most previous launches. While Iran has confirmed the existence of an IRGC space program previously, a launch from the military program had not been reported until April 2020. A successful launch after multiple failures and using new technology signals Iran's intention to press the launch envelope, despite Tehran's insistence that Iran will maintain its self-imposed range limit on missiles.[84]

Third, the Noor-1, via the Qased SLV, was launched from a mobile launcher.[85] The Qased is the first not to be launched from Iran's Imam Khomeini Spaceport, reportedly launching from a mobile transport-erector launcher at the IRGC missile development and launch complex in Shahroud.[86] A mobile launch capability serves little purpose in a civilian satellite program, but it does for a military program concerned about pre-launch strikes.[87] Coupled with Iran's failure to issue any Notice to Airmen (NOTAM) about the launch, the introduction of a mobile launcher lends weight to the claims of space launch being a means to a ballistic missile end.[88]

U.S. defense officials downplayed the success and overall value of the launch.[89] Chief of Space Operations General Raymond, at the time dual-hatted as the commander of the U.S. Space Command, tweeted his view of the satellite as a "tumbling webcam."[90] While independent reporting concurs that the Noor-1 is much too small to be an effective military spy satellite, the advancement in launch capabilities should concern policymakers with what Iran is planning to pursue next.[91]

A New Iranian Rocket, the Zuljanah

ON FEBRUARY 1, 2021, Iran announced that it again tested a new SLV.[92] Called the Zuljanah, it is reported to be able to send a 485-pound satellite into LEO.[93] The Zuljanah features solid-fuel propelled engines in its first and second stages and a liquid-fuel third stage.[94] Though compatible with Iran's mobile launcher, reports indicate that the Zuljanah was launched from the fixed-structure launch pad in Iran's Semnan province.[95] One report cited the seemingly unnecessarily large diameter of the first stage motor, stating it had a thrust of 75 kilotons.[96] This latest test again raises concerns over Iran's ballistic missile aspirations. At the time of this publication, there have been no open-source comments from the U.S. government or its allies about the February launch. An Iranian Defense Ministry Space Department spokesman noted that the first launch of the new SLV was for suborbital testing and will be ready to put operational satellites into orbit after the completion of research tests.[97]

COUNTERSPACE WEAPONS

Kinetic Physical

Current open-source information does not indicate that Iran has or is attempting to develop either direct-ascent or co-orbital ASAT weapons. However, reporting on the April 2020 successful launch and February 2021 test launch brings Iran closer to possessing a future direct-ascent kinetic ASAT capability. Iran must still overcome other technological hurdles before it can field a viable direct-ascent kinetic ASAT weapon. As in last year's report, Iran could threaten satellites by creating a debris hazard in orbit.[98] By placing a small satellite in orbit, Iran demonstrates that it could be closer to developing a co-orbital ASAT weapon. However, it is still unlikely until there is evidence that Iran possesses the more advanced technical means and expertise required to place and maneuver a satellite in orbit to execute such a threat.

Non-kinetic Physical

Current open-source information also does not indicate with any certainty that Iran has made strides in non-kinetic physical weapons in the past year. As with a direct-ascent ASAT capability, Iran's recent launch successes could lead to a greater threat if Iran is also successful in nuclear weapons development.

Electronic

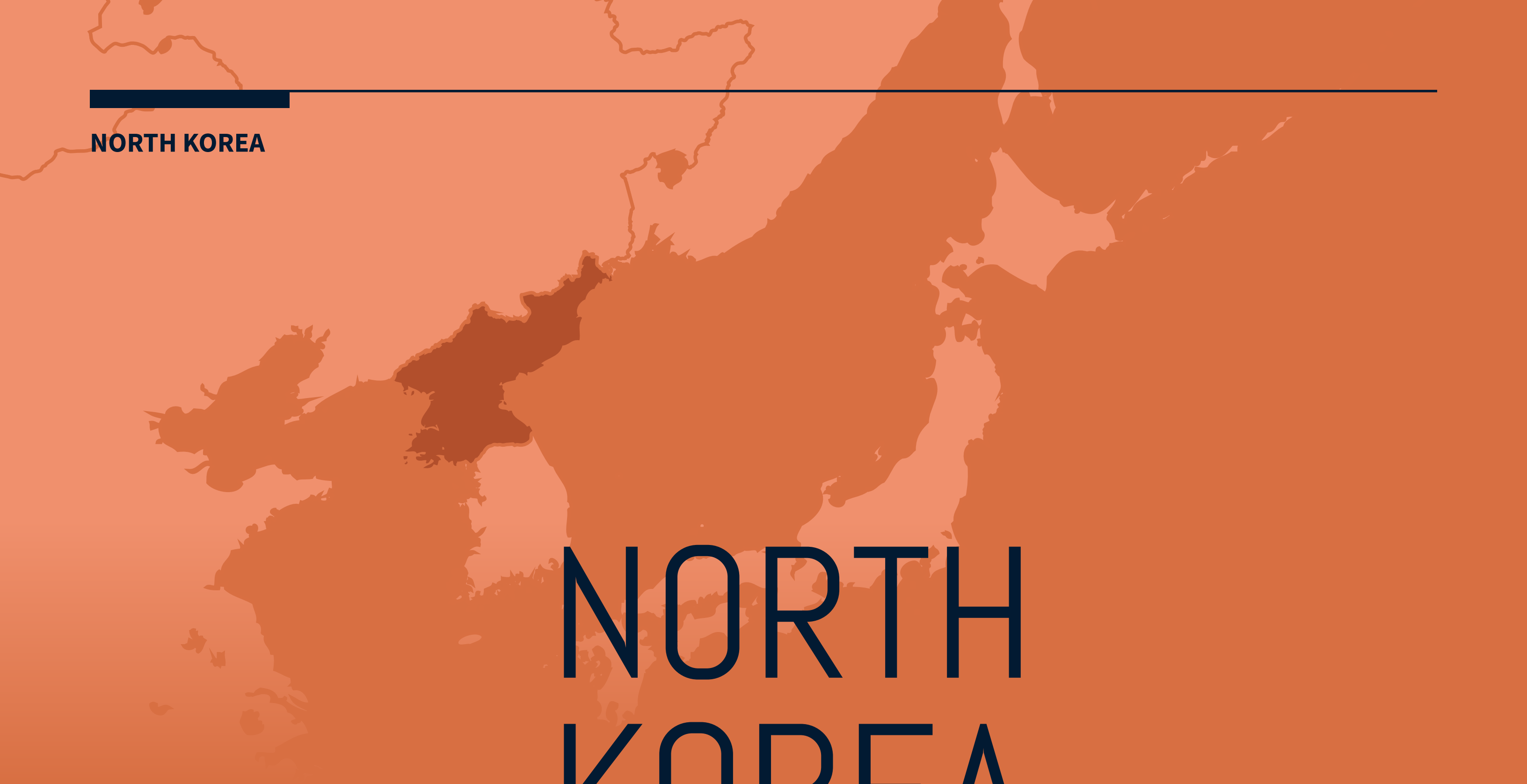
The IRGC conducted two major exercises in 2020, which Iranian sources claim included "space operations" using jamming drones and radar units from the IRGC Aerospace Force.[99] In February 2021, Aerospace Force Brigadier General Mehdi Hadian hailed Iranian electronic warfare capabilities in recent exercises, with a focus on offensive and counter electronic warfare against enemy air power.[100] In March and May 2020, there were reports of Iranian GPS circle spoofing. GPS circle spoofing differs from other spoofing attacks in that it causes transponders to show various erroneous positions forming odd ring-like patterns around a central location.[101] Previously observed in China, the March 2020 incident involved a potential GPS spoofing device in operation at Iran's Army Command and Staff College.[102] The May 2020 incident also involved the circling phenomena with GPS-based reporting systems from vessels and fitness trackers in Tehran.[103] Iran has publicly claimed in the past to have the capability to spoof GPS receivers.[104]

Cyber

Iran has demonstrated its cyber capabilities most prominently this year through its use of civilian cyberattacks against Israel.[105] Past reports suggest that Iran leverages contract hacking groups to conduct cyberattacks on its behalf.[106] In line with this assertion, the Iran-linked Pay2Key hacking group claimed that it hacked a database of Israel Aerospace Industries' subsidiary Elta Systems in December 2020. While Pay2Key is not officially linked to the Iranian government, it is based in Iran and matches the modus operandi of previous Iranian cyberattacks.[107] That same month, the U.S. Cybersecurity and Infrastructure Security Agency issued an Iranian hacker warning. The report stated that "Iranian cyber threat actors have been continuously improving their offensive capabilities." Noted threat activities included website defacement, distributed denial of services, theft of personally identifiable information, and use of destructive malware, among other activities.[108]

While there is no recent open-source information of Iranian cyberattacks specifically against space assets, the increase in frequency and sophistication of recent Iranian cyberattack campaigns suggests that cyberattacks on space systems could be the preferred course of action to compensate for the imbalance of capabilities in other domains. Additionally, in January of this year, Iran and Russia signed an information security agreement that signals closer interaction between the two in cybersecurity activities.[109] That agreement could mean that Iran will benefit from Russian technology, expertise, and training to further its own cyberattack capabilities.

THE INCREASE IN FREQUENCY AND SOPHISTICATION OF RECENT IRANIAN CYBERATTACK CAMPAIGNS SUGGESTS THAT CYBERATTACKS ON SPACE SYSTEMS COULD BE THE PREFERRED COURSE OF ACTION



NORTH KOREA

THE PAST YEAR PROVED TO BE A QUIET ONE for North Korea's counterspace pursuits. It remains unlikely that North Korea is capable or actively pursuing direct-ascent or co-orbital ASAT weapons, and there is little indication that North Korea has made any advancement in its non-kinetic physical capabilities, though some sources insist that a North Korean EMP threat exists. North Korea has demonstrated the ability to conduct electronic warfare through jamming capabilities, and its cyberattack threat is active and viable. It is these latter two capabilities that have the greatest potential for counterspace applications. Recent claims that North Korea and Iran have resumed cooperation on missile and launch vehicle technology could suggest that advancement by one nation may eventually be transferable to the other.[110]

SPACE ORGANIZATION

North Korea continues its claims of peaceful intentions in space, despite a UN Security Council report labelling North Korea's space program a threat to international peace.[111] In May 2020, North Korean state television aired a segment on the National Aerospace Development Administration (NADA) to promote the nation's space program.[112] Pyongyang's propaganda service, Naenara, stated that the purpose of North Korea's space program is to "adhere to the interests of the state and to use science and technology to solve

IT IS WIDELY SUSPECTED THAT NORTH KOREA'S SPACE INTENTIONS ARE CLOSELY TIED TO ITS BALLISTIC MISSILE ASPIRATIONS.

scientific and technological problems essential to economic construction and people's lives."[113] However, much like in the case of Iran, it is widely suspected that North Korea's space intentions are closely tied to its ballistic missile aspirations.

SPACE LAUNCH CAPABILITIES

North Korea maintains two established launching areas for space capabilities: the Tonghae Satellite Launching Ground and the Sohae Satellite Launching Ground. No open-source information emerged in the past year regarding use of the Tonghae site. The website 38 North published imagery and analysis three times since March 2020 reporting normal maintenance, snow clearing, and routine activity, but nothing to indicate the preparation for or execution of a launch in the past year.[114] North Korea also has a General Satellite Control Building (GSCB) intended to track and monitor its own satellite launches and orbiting satellites.[115] Reports indicate the ongoing construction of what is believed to be new scientific testing facilities next to the GSCB, though it is unclear what the exact purpose of those facilities will be.[116]

COUNTERSPACE WEAPONS

Kinetic Physical

No recent open-source information indicates that North Korea has or is attempting to develop a dedicated direct-ascent ASAT program apart from its ongoing ballistic missile programs.[117] North Korean leader Kim Jong Un proclaimed in January 2021 that North Korea will build a solid-fuel intercontinental ballistic missile.[118] It is conceivable that if North Korea achieved this it could leverage that technology to pursue a complementary direct-ascent ASAT capability. However, lacking the means to guide the warhead to directly strike a satellite, the best North Korea could hope to achieve is a broad area weapon meant to create a dangerous debris hazard for orbiting satellites.[119]

Likewise, North Korea does not appear to be pursuing a co-orbital ASAT weapon. To date, North Korea has not demonstrated the means and expertise to conduct RPOs or active guidance measures required for a viable co-orbital ASAT capability.[120] With only a handful of North Korean objects currently in space, and minimal activity at its two launch facilities, it is unlikely that North Korea is actively pursuing either direct-ascent or co-orbital ASAT capabilities.

Non-kinetic Physical

No recent open-source information indicates that North Korea has made any advancements in non-kinetic physical ASAT weapons. Some reports highlight the potential for North Korea to place a nuclear weapon on a long-range missile, giving it the capability to create a high-altitude EMP effect.[121] However, there has been no reported activity in the past year to indicate that North Korea is actively pursuing that capability.

Electronic

North Korea continues to exercise its downlink jamming capabilities. In April 2020, North Korea announced that it was preparing to deploy a new "GPS jamming device" for use against South Korea.[122] There have been multiple reports in the past year, as recent as January 2021, that North Korea continues to conduct jamming operations along the peninsula. Many open-source reports in the past year highlight jamming focused on commercial radio broadcast frequencies and civilian GPS signals rather than military targets.[123] The U.S. Army published a new manual titled North Korean Tactics in July 2020 which details North Korea's electronic warfare organizations, capabilities, techniques, and tactics.[124] It highlights the Electronic Warfare Jamming Regiment focused on electronic jamming and signals reconnaissance.[125]

Cyber

According to government officials, the greatest North Korean counterspace threat to the United States is a cyberattack. North Korean Tactics calls out North Korea's elite cyber warfare unit, the Cyber Warfare Guidance Unit, which is also known as Bureau 121. The Army manual claims that Bureau 121 consists of more than 6,000 members, with many operating outside of North Korea in countries such as China, Russia, India, Malaysia, and Belarus.[126]

Former secretary of state Mike Pompeo claimed in December 2020 that North Korea posed a greater threat to U.S. cybersecurity than Russia.[127] This sentiment was echoed by the current administration in February 2021, as State Department spokesman Ned Price noted that North Korea's malicious cyber activities threatening the United States and its allies will inform an ongoing review of U.S. policy toward North Korea.[128]

North Korea is also suspected of conducting cyberattacks targeted at cybersecurity researchers.[133] The attacks, reported by Google researchers in January 2021, involved sophisticated social media deception and phishing techniques to entice researchers to click links containing malicious code designed to give hackers full access to the victim's computer.[134]

While North Korea's cyberattacks have not been specifically targeted at space systems, they demonstrate North Korea's continued focus on developing more sophisticated and viable cyber capabilities. As North Korean hackers acquire more advanced technology, likely through illicit means, and gain experience and expertise, threats to U.S. space systems and ground stations will become more credible.

North Korean Cyber Profiteering

THE U.S. JUSTICE DEPARTMENT CHARGED three North Korean computer programmers, identified by prosecutors as members of a North Korean military intelligence agency, with carrying out a broad range of global hacks at the behest of the North Korean government.[129] According to the report, it is believed that the defendants executed a number of cyberattacks from locations in Russia and China.[130] The hacks were primarily profit-driven, believed to be intended to offset sanctions against North Korea. This aligns with a report to the UN Security Council detailing North Korean-linked cyber actors conducting operations against financial institutions and virtual currency exchange houses to "generate money to support its weapons of mass destruction and ballistic missile programs."[131] The report contended that North Korea's "total theft of virtual assets from 2019 to November 2020 is valued at approximately $316.4 million."[132]

INDIA

SINCE LAUNCHING ITS FIRST SATELLITE IN 1980, India has shown progressive growth in its space capabilities. With a successful ASAT test in 2019, India became only the fourth country to demonstrate a kinetic counterspace capability. India is also advancing its civil space program, which is currently working on its third mission to the Moon.

SPACE ORGANIZATION

India's space activities are bifurcated into civil and military space organizations. All civil space developments fall under the Indian Space Research Organisation (ISRO), which operates under the Department of Space.[135] The agency celebrated its 51st launch in November 2020, its only launch of 2020, due to the Covid-19 pandemic.[136] India's first orbital launch of 2021 was on February 28, when the country successfully delivered a total of 19 satellites into orbit, including a Brazilian Earth observation satellite.[137]

In 2019, India created the Defence Space Research Organisation (DSRO), which is charged with the research and development of national security space systems and operates under the Defence Space Agency in the Ministry of Defence. These new agencies are part of India's larger goals of advancements in strategic space operations. At its creation, the DSRO was tasked with developing "space warfare systems" and technology.[138] Many Indian counterspace capabilities are developed to respond to security threats posed by China and Pakistan.[139]

India has also been working with private companies to provide SDA data to "detect, identify, and track enemy assets." According to a request for information, the Defence Space Agency is hoping that, once developed, the system can play both defensive and offensive roles.[140]

THESE NEW AGENCIES ARE PART OF INDIA'S LARGER GOALS OF ADVANCEMENTS IN STRATEGIC SPACE OPERATIONS.

COUNTERSPACE WEAPONS

Kinetic Physical

After a successful direct-ascent ASAT test in March 2019, India has not conducted additional public demonstrations of any kinetic physical counterspace weapons. Satheesh Reddy, head of DRDO, stated that while the 2019 direct-ascent ASAT test was at a low altitude to prevent large amounts of space debris, the missile would be capable of reaching most satellites in LEO. A second kinetic test does not seem likely for the country, but Reddy announced that the team was working on technologies related to EMP capabilities and co-orbital weapons.[141]

Non-kinetic Physical

There have not been any publicly reported developments of India's non-kinetic physical capabilities, though there is reason to believe they are being developed. In late 2020, Reddy announced a program to begin development of directed energy weapons, specifically high-energy lasers and high-powered microwaves which could in theory be adapted as counterspace weapons. Though most of these weapons are in the early stages of development, there are two systems which have lasers capable of striking short-range aerial targets, most likely drones. One system is trailer-mounted, the other is tripod-mounted, and both are capable of jamming command and control links to close-range aerial targets.[142] The DRDO has a subsection called the Laser Science and Technology Centre, the website for which specifies work on developing "high power laser sources and related technologies for directed energy applications" as well as "laser countermeasure systems."[143] Though there are no indications of fully functional counterspace systems yet, these reports indicate that high-powered lasers and directed energy technologies with potential counterspace applications are in development.

Electronic

The DRDO provides electronic warfare capabilities for the Indian military. One of India's most used systems is the fully mobile Samyukta electronic warfare system, which is used for surveillance, interception, position fixing, and jamming of communications and radar signals in a wide range of wavelengths.[144] Another fully developed electronic warfare system is the ground vehicle-based Himshakti, reportedly the most powerful electronic warfare system in India's arsenal. It is designed to be used as an offensive and defensive system and can jam frequencies over an area as large as 10,000 square kilometers.[145] It is reported that India was able to jam Pakistani radars and communication during a 2019 airstrike, though it is not clear which system was used.[146]

Cyber

India has continued to develop its Defense Cyber Agency, which responds to threats in the cyber domain.[147] As the country's cyber capabilities grow, its most frequent targets are the governments of Pakistan and China.[148] Based on open-source information, it does not appear that India has tested or used its cyber capabilities against space systems.

OTHERS

WHILE CHINA, RUSSIA, IRAN, NORTH KOREA, AND INDIA have the most public advancements in counterspace weapons, other states are developing counterspace capabilities as well. This chapter examines the counterspace applications that other countries possess, including U.S. allies and partners, and include public remarks and changes in doctrine.

"... There's a realization amongst nations that access to space is no longer a given. We've got to make sure that we stay ahead of this growing threat."

– GENERAL JOHN RAYMOND, CHIEF OF SPACE OPERATIONS, U.S. SPACE FORCE[149]

FRANCE

After issuing a new Space Defense Strategy in 2019, France has had a continued focus on military space. In March of 2021, the French Space Command began a simulated "stress test" of existing systems, in what the French commander, Major General Michel Friedling, denoted as a "first for the French army and even a first in Europe." These simulations reportedly included "monitoring of a potentially dangerous space object, as well as a threat to a satellite." The drills lasted five days and included participation from the U.S. Space Force and German space agencies.[150]

ISRAEL

As reported last year, Israel has continued development of a laser defense system called the Iron Beam, which can intercept lower-tier rockets and missiles. Israel's Ministry of Defense has announced land, sea, and air systems to compliment the laser.[151] Israel has also developed a smaller laser defense weapon, Light Blade, that can target balloons or kites up to two kilometers in the distance.[152] Continued developments and investments in laser technology used on Earth are a step closer to counterspace laser technology; however, there are many additional technical challenges for lasing a satellite from Earth that Israel has not yet demonstrated.

JAPAN

Japan continues to advance its civil and military space operations. Prior to the passage of the 2008 Basic Space Law, Japan had a national policy that prohibited the use of space for national defense.[153] The 2008 law permitted the country to begin military developments in space, and government officials have begun to speak out about the development of defensive counterspace capabilities.[154] The timing of this law and the ramping up of many counterspace developments are in response to actions by China in space, such as the 2007 Chinese debris-producing ASAT test.

This year, Japan authorized a bill to set up its proposed Space Domain Mission Unit within the Japan Air Self-Defense Force. The squadron is slated to be fully operational by 2023, with plans to launch the first satellite for monitoring the space environment by 2026.[155] The Space Operations Squadron was established in 2020 as the first space domain mission unit with the official mission to protect Japanese satellites from damage, including armed attacks, and to monitor the space environment, including space debris, asteroids, and other satellites. The Space Operations Squadron will cooperate with U.S. Space Command and Japan's civil agency, the Japan Aerospace Exploration Agency. Yasuhito Fukushima, a senior research fellow at the Japanese National Institute for Defense Studies, added that "Japan's security space activities are premised on cooperation with the United States."[156]

While Japan has not demonstrated any direct-ascent ASAT systems, the country has U.S.-made SM-3 missile defense interceptors that have a latent ability to attack space assets in LEO. Because military developments in space are relatively new to the country, most public remarks have been about the possibility of capabilities that the country is interested in pursuing, such as co-orbital ASAT and jamming capabilities. In 2020, then-prime minister Shinzo Abe declared that the country will "drastically bolster capability and systems in order to secure superiority," though no specific programs have been made public.[157]

SOUTH KOREA

In an October 2020 blog post, the government of South Korea discussed its need to reinforce satellite navigation with terrestrial systems to combat jamming and spoofing. The country cited its past troubles with spoofing from North Korea, specifically from 2010 to 2016, as a driving force to augment GPS use with terrestrial systems.[158] The Ministry of Science also released a statement detailing plans to upgrade space capabilities, including the launch of the first locally built rocket that will carry satellites and orbiter probes to the Moon, with aims for a more powerful rocket by 2029.[159]

UNITED KINGDOM

The United Kingdom continues to integrate space into its military structure. In 2021, the country announced its largest defense budget since the Cold War, a portion of which will go toward building the Royal Air Force Space Command in Scotland. The first commander of the United Kingdom's Space Command was announced in February 2021, and the command is scheduled to be operational and capable of launching its first rocket by 2022.[160] Space Command will work alongside the Ministry of Defence's recently formed Space Directorate as a joint command structure.[161]

CONTINUED DEVELOPMENTS AND INVESTMENTS IN LASER TECHNOLOGY USED ON EARTH ARE A STEP CLOSER TO COUNTERSPACE LASER TECHNOLOGY.

WHAT TO WATCH

THE COMING YEAR MAY BE MARKED MORE BY THE CONTINUITY of current trends rather than any disruptive changes. While China continues to make progress in developing counterspace weapons, its focus appears to be shifting to integrating these capabilities into its forces and operational plans. A key issue to watch over the coming year is China's overall investment in space-related research and development and the development of potentially dual-use space capabilities, such as its tentacle space debris cleanup robot. From an operational perspective, a key development to track is the progress China makes integrating its electronic counterspace capabilities, such as jamming and spoofing, into its irregular warfare forces and tactics. In terms of norms of behavior in space, a key indicator to watch is the behavior of China's SJ-17 GEO inspector satellite. While SJ-17 appears to have focused on inspecting other Chinese satellites so far, using this satellite to inspect another nation's satellites in GEO would mark an important shift in its use that could have broader repercussions.

Russia is perhaps the most likely nation to conduct additional counterspace testing and deployment over the coming year. Given the tests of its direct ascent and co-orbital ASAT weapons conducted in 2020, a key issue to watch is whether these tests continue and if new capabilities are demonstrated. Other areas to watch for Russia include tests of new direct ascent or co-orbital ASAT capabilities, laser ASAT systems on additional airborne and ground-based platforms, electronic warfare systems for the protection of critical platforms, and emboldened cyberattacks against civilian infrastructure and government institutions.

Both Iran and North Korea continue to have relatively immature space capabilities, but their electronic and cyber counterspace capabilities pose a serious threat. Over the coming year, Iran will likely continue its space launch activities under the IGRC and North Korea may look to restart testing of its space launch capabilities after a year of relative dormancy. A key development to watch is any additional indication that Iran and North Korea are cooperating in space or ballistic missile technology, which could mean progress in one country is likely to be transferred to the other. Additional issues to watch include continued Iranian GPS spoofing in the Persian Gulf and North Korean GPS jamming into South Korea. An increased frequency and sophistication of cyberattacks by either country in other domains could also indicate a higher level of cyber threats to space systems.

India does not appear to be poised to conduct another test of its direct ascent ASAT missile in the near future. It is more likely to continue development of high-powered lasers and other non-kinetic ASAT capabilities. Key indicators for India in space include how its new military and research and development space agencies continue to develop, the level of funding provided for space and counterspace activities, and signs that it is adapting or testing its electronic warfare systems for use against space systems.

Overall, 2020 was a slow year for counterspace activities, with a few notable exceptions detailed in this year's report. The coming year may prove more active overall as nations reemerge from lockdown and return to their prior plans and programs. As the new U.S. administration develops and refines its overall national security strategy, one of the key areas to watch will be how it addresses space policy issues in general and the proliferation of counterspace weapons. Calls within the United States and abroad for more clearly defined norms of behavior in space are growing.[162] An early indication that the Biden administration intends to make progress toward building norms in space would be an agreement among DoD and the intelligence community for which norms the U.S. government is willing to support and abide by. Without an interagency agreement within the U.S. government, it will be difficult to start a meaningful conversion with other governments.

2020 WAS A SLOW YEAR FOR COUNTERSPACE ACTIVITIES, WITH A FEW NOTABLE EXCEPTIONS.

ABOUT THE AUTHORS

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

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

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

LIEUTENANT COLONEL JOE MOYE is an active-duty Marine Corps officer with nearly 22 years of service. He graduated from Appalachian State University in 1998 with a bachelor's degree in criminal justice and commissioned in 1999. He holds a master's degree in international public policy from the Johns Hopkins School of Advanced International Studies, with a strategic studies concentration. His operational assignments include a marine expeditionary unit afloat and six deployments to the Middle East, the African Continent, and European Theater. His most recent operational assignment was battalion command in Camp Lejeune, North Carolina. His Marine Corps staff positions include Marine Corps Forces Special Operations Command and Headquarters, Marine Corps. His joint assignments include United States Special Operations Command, Special Operations Joint Task Force/NATO Special Operations Component Command - Afghanistan, and Transregional Threats Coordination Cell, Joint Staff J5 Directorate.

MAKENA YOUNG is a research associate with the Aerospace Security Project at 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.

ENDNOTES

INTRODUCTION

1 "UCS Satellite Database," Union of Concerned Scientists, accessed February 26, 2021, https://www.ucsusa.org/resources/satellite-database.

2 Makena Young, "How Does Space Policy Directive-5 Change Cybersecurity Principles for Space Systems?," Aerospace Security, September 14, 2020, https://aerospace.csis.org/how-does-space-policy-directive-5-change-cybersecurity-principles-for-space-systems/.

3 "Memorandum on the National Strategy for Space Nuclear Power and Propulsion (Space Policy Directive-6)," White House, December 16, 2020, https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-national-strategy-space-nuclear-power-propulsion-space-policy-directive-6/; and "Memorandum on Space Policy Directive 7," White House, January 15, 2021, https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-7/.

4 "NASA Administrator Signs Statement of Intent with Brazil on Artemis Cooperation," NASA, December 14, 2020, https://www.nasa.gov/feature/nasa-administrator-signs-statement-of-intent-with-brazil-on-artemis-cooperation.

5 Todd Harrison and Seamus P. Daniels, Analysis of the FY 2021 Defense Budget (Washington, DC: CSIS, August 2020), 45-49, https://defense360.csis.org/analysis-of-the-fy-2021-defense-budget/.

6 U.S. Space Force, Spacepower: Doctrine for Space Forces (Washington, DC: August 2020), https://www.spaceforce.mil/Portals/1/Space%20Capstone%20Publication_10%20Aug%202020.pdf.

7 U.S. Space Command, Commander's Strategic Vision (Washington, DC: January 2021), https://www.spacecom.mil/Portals/32/Images/cc-vision/usspacecom-strategic-vision-22feb21.pdf?ver=xW4jfruY-cHS0HfWf6KN9A%3d%3d.

TYPES OF COUNTERSPACE WEAPONS

8 U.S. Space Force, Spacepower, 43.

9 "Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space, and Under Water," Department of State, https://2009-2017.state.gov/t/avc/trty/199116.htm#signatory.

10 Brian Garino and Jane Gibson, "Space System Threats," in AU-18 Space Primer (Maxwell Air Force Base, AL: Air University Press, September 2009), 277, http://space.au.af.mil/au-18-2009/au-18_chap21.pdf.

11 Richard B. Langley et al., "Innovation: GNSS Spoofing Detection," GPS World, June 1, 2013, http://gpsworid.com/innovation-gnss -spoofing-detection-correlating-carrier-phase-with-rapid-antenna-motion/.

CHINA

12 "Counterspace Weapons Timeline," Aerospace Security, accessed March 25, 2021, https://aerospace.csis.org/counterspace-timeline.

13 Leonard David, "China's Chang'e 5 moon samples are headed to the lab," Space.com, December 18, 2020, https://www.space.com/china-chang-e-5-moon-samples-lab.

14 "China's Chang'e-4 probe resumes work for 27th lunar day," Xinhua, February 2, 2021, http://www.xinhuanet.com/english/2021-02/07/c_139727894.htm.

15 Stephan Clark, "China to begin construction of space station this year," Spaceflight Now, January 10, 2021, https://spaceflightnow.com/2021/01/10/china-to-begin-construction-of-space-station-this-year/.

16 Leonard David, "China's Tianwen-1 Mars mission adjusts orbit to prepare for a Red Planet landing," Space.com, February 17, 2021, https://www.space.com/china-tianwen-1-mars-mission-adjusts-orbit-for-landing.

17 Joseph Trevithick and Tyler Rogoway, "China's Secret Spacecraft Looks To Have Landed At This Remote Base With A Massive Runway," The Drive, September 8, 2020, https://www.thedrive.com/the-war-zone/36270/this-remote-base-with-a-massive-runway-looks-to-be-where-chinas-secretive-spacecraft-landed.

18 Geoff Brumel, "New Chinese Space Plane Landed At Mysterious Air Base, Evidence Suggests," NPR, September 9, 2020, https://www.npr.org/2020/09/09/911113352/new-chinese-space-plane-landed-at-mysterious-air-base-evidence-suggests.

19 Andrew Jones, "China's CASIC reveals five-year plan for reusable spaceplane, commercial space projects," *SpaceNews,* October 19, 2020, https://spacenews.com/chinas-casic-reveals-five-year-plan-for-reusable-space-plane-commercial-space-projects/.

20 "China puts final satellite into orbit to try to rival GPS network," Reuters, June 22, 2020, https://www.reuters.com/article/us-space-explora-

tion-china-satellite/china-puts-final-satellite-into-orbit-to-try-to-rival-gps-network-idUSKBN23U08P.

21 "Beidou Global Navigation Satellite System," Glonass, accessed February 26, 2021, https://www.glonass-iac.ru/en/guide/beidou.php.

22 Andrew Jones, "China successfully launches new Long March 7A on second attempt," *SpaceNews*, March 11, 2021, https://spacenews.com/china-successfully-launches-new-long-march-7a-on-second-attempt/.

23 John Costello and Joe McReynolds, China's Strategic Support Force: A Force for a New Era (Washington, DC: Institute for National Strategic Studies, October 2018), 10-12, 15, 16, https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.

24 Alexander Bowe, "China's Pursuit of Space Power Status and Implications for the United States," U.S.-China Economic and Security Review Commission, April 11, 2019, https://www.uscc.gov/sites/default/files/Research/USCC_China's%20Space%20Power%20Goals.pdf.

25 "Counterspace Weapons Timeline," Aerospace Security, accessed March 25, 2021, https://aerospace.csis.org/counterspace-timeline.

26 This approximation was derived from the formula: distance(km) = 2 * orbital radius * SIN (0.5*angular separation).

27 Thomas G. Roberts, "Unusual behavior in GEO: SJ-17," Aerospace Security, March 30, 2020, https://aerospace.csis.org/data/unusual-behavior-in-geo-sj-17/.

28 "China develops new tentacle-like robot to clear space debris," Xinhua, February 4, 2021, http://www.xinhuanet.com/english/2021-02/04/c_139721266.htm.

29 Brian G. Chow and Henry Sokolski, "U.S. Satellites Increasingly Vulnerable to China's Ground Based Lasers," *SpaceNews*, July 10, 2020, https://spacenews.com/op-ed-u-s-satellites-increasingly-vulnerable-to-chinas-ground-based-lasers/.

30 Shishir Gupta, "China builds new structures near LAC, relocates troops. India reads a message," *Hindustan Times*, October 24, 2020, https://www.hindustantimes.com/india-news/india-spots-movement-across-lac-china-is-building-new-structures-relocating-troops/story-DIe6zUzawUyTwEBrakZ45K.html.

RUSSIA

31 "Aerospace Defence Forces," Space Forces: Ministry of Defence of the Russian Federation, https://eng.mil.ru/en/structure/forces/cosmic.htm; and Matthew Bodner, "As Trump Pushes for Separate Space Force, Russia Move Fast the Other Way," Defense News, June 22, 2018, https:// www.defensenews.com/global/europe/2018/06/21/as-trump-pushes-for-separate-space-force-russia-moves-fast-the-other-way/.

32 "Russia to Launch 29 Space Rockets in 2021, Says Roscosmos Chief," TASS, February 20, 2021, https://tass.com/science/1259053.

33 "Russian Space Agency Publishes Declassified Documents on World's 1st Lunar Soft Landing," TASS, February 12, 2021, https://tass.com/science/1255965.

34 "Roscosmos Continues Discussing Joint Moon Base with China," TASS, January 25, 2021, https://tass.com/science/1248511.

35 Andrew Jones, "Russia, China to Sign Agreement on International Lunar Research Station," *SpaceNews,* February 17, 2021, https://spacenews.com/russia-china-to-sign-agreement-on-international-lunar-research-station/.

36 Jessie Yeung, "China and Russia agree to build joint lunar space station," CNN, March 10, 2021, https://www.cnn.com/2021/03/09/asia/russia-china-lunar-station-intl-hnk-scli-scn/index.html.

37 Anatoly Zak, "The Angara Family of Launch Vehicles," Russianspaceweb.com, https://russianspaceweb.com/angara.html.

38 "Roscosmos Reaches Agreements to Build Satellites for Several Countries," TASS, January 28, 2021, https://tass.com/science/1250283.

39 代艳 , "Russia Seeks to Counter Space Threats," Chinadaily.com.cn, June 4, 2020, http://global.chinadaily.com.cn/a/202006/04/WS5ed85870a310a8b24115ac9c.html.

40 "Russia Tests Direct-Ascent Anti-Satellite Missile," United States Space Command, April 15, 2020, https://www.spacecom.mil/MEDIA/NEWS-ARTICLES/Article/2151611/russia-tests-direct-ascent-anti-satellite-missile/.

41 Kyle Mizokami, "Meet Russia's Imposing New Satellite-Destroying Missile," *Popular Mechanics,* April 16, 2020, https://www.popularmechanics.com/military/weapons/a32173824/nudol-missile-anti-satellite/.

42 Sandra Erwin, "Space Force Official: Russian Missile Tests Expose Vulnerability of Low-Orbiting Satellites," *SpaceNews*, December 17, 2020, https://spacenews.com/space-force-official-russian-missile-tests-expose-vulnerability-of-low-orbiting-satellites/.

43 Pavel Podvig, "Nudol ASAT System Tested from Plesetsk," Russian Strategic Nuclear Forces, December 16, 2020, http://russianforces.org/blog/2020/12/nudol_asat_system_tested_from.shtml.

44 "Russia Conducts Space-Based Anti-Satellite Weapons Test," United States Space Command, July 23, 2020, https://www.spacecom.mil/MEDIA/NEWS-ARTICLES/Article/2285098/russia-conducts-space-based-anti-satellite-weapons-test/.

45 "Kosmos 2519 / Kosmos 2521 / Kosmos 2523," Gunter's Space Page, https://space.skyrocket.de/doc_sdat/kosmos-2519.htm.

46 Beyza Unal, "Russia's Behaviour Risks Weaponizing Outer Space," Chatham House, July 31, 2020, https://www.chathamhouse.org/2020/07/

russias-behaviour-risks-weaponizing-outer-space.

47 “Russia Committed to Full Demilitarization of Outer Space, Kremlin Says,” TASS, July 24, 2020, https://tass.com/politics/1181997.

48 Jonathan McDowell, Twitter Post, June 15, 2020, 12:30 pm,https://twitter.com/planet4589/status/1272567228416827395?lang=en.

49 Anatoly Zak, “Soyuz-2-1v Launches Four Classified Payloads,” Russianspaceweb.com, http://russianspaceweb.com/Cosmos-2535-2536-2537-2538.html.

50 Peter Suciu, “S-500: Russia’s F-35 Killer Coming Next Year,” *National Interest,* November 30, 2020, https://nationalinterest.org/blog/buzz/s-500-russias-f-35-killer-coming-next-year-173514.

51 “Russia Touts S-500’s Ability to Destroy Hypersonic Weapons in Space,” Moscow Times, March 5, 2021, https://www.themoscowtimes.com/2020/07/03/russia-touts-s-500s-ability-to-destroy-hypersonic-weapons-in-space-a70767.

52 “Is the S-500 Russia’s Answer to America’s Space Corps? Hypersonic Missile System Designed to Intercept Attacks from Space,” Military Watch Magazine, July 8, 2019, https://militarywatchmagazine.com/article/is-the-s-500-russia-s-answer-to-america-s-space-corps-hypersonic-missile-system-designed-to-intercept-attacks-from-space.

53 Joseph Trevithick, “Here’s Our Best Look Yet at Russia’s Secretive Space Cannon, The Only Gun Ever Fired in Space,” The Drive, February 16, 2021, https://www.thedrive.com/the-war-zone/39277/heres-our-best-look-yet-at-russias-secretive-space-cannon-the-only-gun-ever-fired-in-space.

54 Bart Hendrickx, “Peresvet: a Russian Mobile Laser System to Dazzle Enemy Satellites,” The Space Review, June 15, 2020, https://www.thespacereview.com/article/3967/1.

55 John Pike, “A-60 Ladoga 1A Airborne Laser,” https://www.globalsecurity.org/military/world/russia/a-60.htm.

56 Hendrickx, “Peresvet.”

57 Bart Hendrickx, “Russia Gears up for Electronic Warfare in Space (Part 1),” The Space Review, October 26, 2020, https://www.thespacereview.com/article/4056/1.

58 Ibid.

59 Ibid.

60 Ibid.

61 Anatoly Zak, “Lotos-S spacecraft for the Liana system,” Russianspaceweb.com, http://www.russianspaceweb.com/liana.html; and “Liana Electronic Intelligence Program,” Spaceflight101, https://spaceflight101.com/spacecraft/liana-electronic-intelligence-program/.

62 “Liana - Lotus C and Pion-NCC,” GlobalSecurity.org, https://www.globalsecurity.org/space/world/russia/liana.htm.

63 Bart Hendrickx, “Russia Gears up for Electronic Warfare in Space (Part 2),” The Space Review, November 2, 2020, https://www.thespacereview.com/article/4060/1.

64 Ibid.

65 Terry Thompson, “The SolarWinds Hack Was All but Inevitable – Why National Cyber Defense Is a ‘Wicked’ Problem and What Can Be Done about It,” The Conversation, February 9, 2021, https://theconversation.com/the-solarwinds-hack-was-all-but-inevitable-why-national-cyber-defense-is-a-wicked-problem-and-what-can-be-done-about-it-153084.

66 Jason Murdock, “Who Has Been Affected by the Huge SolarWinds Cyberattack so Far?,” *Newsweek,* December 18, 2020, https://www.newsweek.com/solarwinds-orion-software-cyberattack-hack-victims-targets-list-1555840; and David E. Sanger, Nicole Perlroth, and Julian E. Barnes, “As Understanding of Russian Hacking Grows, So Does Alarm,” New York Times, January 2, 2021, https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.

67 Ibid.

68 Andy Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History,” *Wired,* August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/; and “Global Ransomware Attack Causes Turmoil,” BBC News, June 28, 2017, https://www.bbc.com/news/technology-40416611.

IRAN

69 Samuel Hickey, “Iran’s military satellite launch: What just happened?,” Center for Arms Control and Non-Proliferation, May 4, 2020, https://armscontrolcenter.org/irans-military-satellite-launch-what-just-happened/; “Iran Lying About Peacefulness of Space Program, Pompeo Says,” Radio Farda, April 25, 2020, https://en.radiofarda.com/a/iran-lying-about-peacefulness-of-space-program-pompeo-says/30576344.html; “US Calls On Europe, Others To Take Action Against Iran After Satellite Launch,” Radio Farda, April 26, 2020, https://en.radiofarda.com/a/us-calls-on-europe-others-to-take-action-against-iran-/30577148.html; and “UK Says Iran’s ballistic missile launch is of significant concern,” Reuters, April 24, 2020, https://www.reuters.com/article/us-iran-satellite-britain/uk-says-irans-ballistic-missile-launch-is-of-significant-concern-idUSKCN2261JA.

70 Andrew Hanna, “Iran’s Ambitious Space Program,” The Iran Primer, Updated February 1, 2021, https://iranprimer.usip.org/blog/2020/jun/23/iran%E2%80%99s-ambitious-space-program; and Shaul Shay, “Iran and the Middle East space race,” *Israel Hayom,* May 4, 2020, https://www.israelhayom.com/opinions/__trashed-7/.

71 “سازمان فضایی ایران,”Iranian Space Agency, July 9, 2016, https://www.isa.ir/find.php?item=1.66.10.fa; and“Space Industry Development Requires National Willpower: Minister,”*Tehran Times,* May 26, 2018, https://www.tehrantimes.com/news/423935/Space-industry-development-requires-national-willpower-minister.

72 Fabian Hinz, “Have Iran’s space ambitions taken a worrisome turn?,” European Leadership Network, April 24, 2020, https://www.europeanleadershipnetwork.org/commentary/have-irans-space-ambitions-taken-a-worrisome-new-turn/.

73 Anthony Cordesman, Iran and the Changing Military Balance in the Gulf (Washington, DC: CSIS, March 2019), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200326_Iran_Gulf_Net_Assesment.Third_Phase.Reduced.GH6%281%29.pdf.

74 “Iran Unveils Military Space Command, New Details on Satellite Launch,” SpaceWatch.Global, April 27, 2020, https://spacewatch.global/2020/04/iran-unveils-military-space-command-new-details-on-satellite-launch/.

75 Marcia Smith, “Iran Launches First Military Satellite From New Launch Site,” Space Policy Online, April 23, 2020, https://spacepolicyonline.com/news/iran-launches-first-military-satellite-from-new-launch-site/; Fabian Hinz, “Have Iran’s space ambitions taken a worrisome turn?,” European Leadership Network, April 24, 2020, https://www.europeanleadershipnetwork.org/commentary/have-irans-space-ambitions-taken-a-worrisome-new-turn/; and Samuel Hickey, “Iran’s military satellite launch: What just happened?,” Center for Arms Control and Non-Proliferation, May 4, 2020, https://armscontrolcenter.org/irans-military-satellite-launch-what-just-happened/.

76 Peter Pry, “Iran’s Satellite is No ‘Tumbling Webcam’,” Newsmax, May 5, 2020, https://www.newsmax.com/peterpry/irgc-sputnik-emp-space/2020/05/05/id/966149/.

77 Marcia Smith, “Iran Launches First Military Satellite From New Launch Site,” Space Policy Online, April 23, 2020, https://spacepolicyonline.com/news/iran-launches-first-military-satellite-from-new-launch-site/.

78 Ibid.

79 “Guards Commander Says Iran’s Eye in the Sky Makes it a ‘A World Power’,” Radio Farda, April 22, 2020, https://en.radiofarda.com/a/guards-commander-says-iran-s-eye-in-sky-makes-it-a-world-power-/30570301.html.

80 Jeremy Binnie, “US SPACECOM Commander Dismisses Iranian ‘Webcam’ Satellite,” Janes, April 30, 2020, https://www.janes.com/defence-news/news-detail/us-spacecom-commander-dismisses-iranian-webcam-satellite; and Pry, “Iran’s Satellite is No ‘Tumbling Webcam.’”

81 Smith, “Iran Launches First Military Satellite From New Launch Site.”

82 Fabian Hinz, “Perspectives on Iran’s Satellite Launch: Fabian Hinz on the Qased Satellite Launch Vehicle,” SpaceWatch.Global, May 13, 2020, https://spacewatch.global/2020/05/spacewatchgl-perspectives-on-irans-satellite-launch-fabian-hinz-on-the-qased-satellite-launch-vehicle/; and Hickey, “Iran’s military satellite launch.”

83 Ibid.

84 Hinz, “Perspectives on Iran’s Satellite Launch.”

85 Hickey, “Iran’s military satellite launch.”

86 Fabian Hinz, “Have Iran’s space ambitions taken a worrisome turn?,” European Leadership Network, April 24, 2020, https://www.europeanleadershipnetwork.org/commentary/have-irans-space-ambitions-taken-a-worrisome-new-turn/.

87 Hickey, “Iran’s military satellite launch.”

88 Smith, “Iran Launches First Military Satellite From New Launch Site.”

89 “Pentagon Official Says Iran Satellite Launch Vehicle Traveled ‘Long Way’,” Radio Farda, April 23, 2020, https://en.radiofarda.com/a/pentagon-official-says-iran-satellite-launch-vehicle-traveled-long-way-/30571984.html.

90 Jay Raymond, Twitter Post, April 25, 2020, 2:19 PM, https://twitter.com/SpaceForceCSO/status/1254158221243277315.

91 Pry, “Iran’s Satellite is No ‘Tumbling Webcam’”; Fabian Hinz, “Have Iran’s space ambitions taken a worrisome turn?”; and Hickey, “Iran’s military satellite launch.”

92 Mihailo Zekic, “Iran Flexes its ‘Space Muscles’ With New Rocket Launch,” Watch Jerusalem, February 9, 2021, https://watchjerusalem.co.il/1162-iran-flexes-its-space-muscles-with-new-rocket-launch; Sune Engel Rasmussen, “Iran Launches New Rocket, Showing Advances in Potential Missile Technology,” Wall Street Journal, February 1, 2021, https://www.wsj.com/articles/iran-launches-new-rocket-showing-advances-in-potential-missile-technology-11612214948; David Axe, “Iran’s New Space Rocket Could Double as a Nuclear Missile,” Forbes, February 1, 2021, https://www.forbes.com/sites/davidaxe/2021/02/01/irans-new-space-rocket-could-double-as-a-weapon/?sh=5e2ec5da2d40; Batya Jerenberg, “Iran tests new ‘most powerful’ rocket capable of carrying nuclear warhead,” Janglo, February 4, 2021, https://www.janglo.net/item/qbkS7rNbA6G; and Elizabeth Howell, “Iran Tests new Rocket on sub-orbital test flight,” Space.com, February 17, 2021, https://www.space.com/iran-tests-new-rocket-zoljanah.

93 Rasmussen, “Iran Launches New Rocket”; and Axe, “Iran’s New Space Rocket”; and Batya Jerenberg, “Iran tests new ‘most powerful’ rocket”; and Howell, “Iran Tests new Rocket on sub-orbital test flight.”

94 Axe, “Iran’s New Space Rocket”; Jerenberg, “Iran tests new ‘most powerful’ rocket”; and Howell, “Iran Tests new Rocket.”

95 Rasanah, “Iran’s Space Dreams are Clear and Dangerous,” International Institute for Iranian Studies, February 16, 2021, https://rasanah-iiis.org/english/monitoring-and-translation/reports/¬irans-space-dreams-are-clear-and-dangerous/.

96 Rasmussen, “Iran Launches New Rocket.”

97 “Iran test launches new domestically manufactured satellite launch vehicle,” Pars Today, February 2, 2021, https://parstoday.com/en/news/iran-i133504-iran_test_launches_new_domestically_manufactured_satellite_launch_vehicle; and Howell, “Iran Tests new Rocket.”

98 Todd Harrison et al., Space Threat Assessment 2020 (Washington, DC: CSIS, March 2020), https://aerospace.csis.org/wp-content/uploads/2020/03/Harrison_SpaceThreatAssessment20_WEB_FINAL-min.pdf.

99 “IRGC launches final stage of joint military exercise in southern Iran,” Iranian Students’ News Agency, July 28, 2020, https://en.isna.ir/news/99050705060/IRGC-launches-final-stage-of-joint-military-exercise-in-southern; “Iran Air Defense forces perform large-scale electronic warfare drills,” Iran Project, October 21, 2020, https://theiranproject.com/blog/2020/10/21/iran-air-defense-forces-perform-large-scale-electronic-warfare-drills/; “Iran launches large-scale electronic aerial drills,” Tehran Times, October 21, 2020, https://www.tehrantimes.com/news/453826/Iran-launches-large-scale-electronic-aerial-drills; “Second day of ‘Velayat-99’ maneuvers performed by Army, IRGC,” Iranian Students’ News Agency, October 22, 2020, https://en.isna.ir/photo/99080100336/Second-day-of-Velayat-99-maneuvers-performed-by-Army-IRGC; and “Massive war games light up Iran’s skies,” Al Monitor, October 21, 2020, https://www.al-monitor.com/pulse/originals/2020/10/iran-war-games-air-defense-exercise-regional-tensions.html.

100 “IRIAF capable of giving ‘prompt’ response to any threat,” Mehr News Agency, February 9, 2021, https://en.mehrnews.com/news/169722/IRIAF-capable-of-giving-prompt-response-to-any-threat.

101 Joseph Trevithick, “New Type of GPS Spoofing Attack in China Creates “Crop Circles” of False Location Data,” The Drive, November 18, 2019, https://www.thedrive.com/the-war-zone/31092/new-type-of-gps-spoofing-attack-in-china-creates-crop-circles-of-false-location-data.

102 Dana Goward, “GPS circle spoofing discovered in Iran,” GPS World, April 21, 2020, https://www.gpsworld.com/gps-circle-spoofing-discovered-in-iran/.

103 Dana Goward, “New GPS ‘circle spoofing’ moves ship locations thousands of miles,” GPS World, May 26, 2020, https://www.gpsworld.com/new-gps-circle-spoofing-moves-ship-locations-thousands-of-miles/.

104 Scott Peterson and Payam Faramarzi,“Exclusive: Iran hijacked U.S. drone, says Iranian engineer,”*Christian Science Monitor*, December 15, 2011, https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer.

105 Gil Baram and Kevin Lim, “Israel and Iran Just Showed Us the Future of Cyberwar with Their Unusual Attacks,” *Foreign Policy,* June 5, 2020, https://foreignpolicy.com/2020/06/05/israel-and-iran-just-showed-us-the-future-of-cyberwar-with-their-unusual-attacks/.

106 Collin Anderson and Karim Sadjadpour, Iran’s Cyber Threat: Espionage, Sabotage, and Revenge (Washington, DC: Carnegie Endowment for International Peace, 2018), https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf; United Against Nuclear Iran, The Iranian Cyber Threat (New York: December 2020), https://www.unitedagainstnucleariran.com/sites/default/files/The%20Iranian%20Cyber%20Threat_1220_JMB_CLEAN.pdf; and Miriam Baksh, “CISA Warns of Iran’s Offensive Cyber Capabilities,” Nextgov, December 4, 2020, https://www.nextgov.com/cybersecurity/2020/12/cisa-warns-irans-offensive-cyber-capabilities/170505/.

107 “Iran-Linked Group Says it Hacked Israeli Aerospace Industries,” Yeshiva World, December 21, 2020, https://www.theyeshivaworld.com/news/headlines-breaking-stories/1930427/iran-linked-group-says-it-hacked-israeli-aerospace-industries.html; and Yossi Mekelberg, “Cyberspace: the new frontier in the Israeli-Iranian battleground,” *Arab News,* December 26, 2020, https://www.arabnews.com/node/1783176.

108 Baksh, “CISA Warns of Iran’s Offensive Cyber Capabilities.”

109 John Hardie and Annie Fixler, “Russia-Iran cooperation poses challenges for US cyber strategy, global norms,” C4ISRNET, February 8, 2021, https://www.c4isrnet.com/thought-leadership/2021/02/08/russia-iran-cooperation-poses-challenges-for-us-cyber-strategy-global-norms/; “Iran, Russia sign information security cooperation pact,” Iranian Students’ News Agency, January 26, 2021, https://en.isna.ir/news/99110705109/Iran-Russia-sign-information-security-cooperation-pact; and “Iran, Russia Ink Cybersecurity Cooperation Pact,” Tasnim News Agency, January 26, 2021, https://www.tasnimnews.com/en/news/2021/01/26/2440530/iran-russia-ink-cybersecurity-cooperation-pact.

NORTH KOREA

110 David Wainer, “Iran and North Korea Resumed Cooperation on Missiles, UN Says,” *Bloomberg,* February 8, 2021, https://www.bloomberg.com/news/articles/2021-02-08/iran-and-north-korea-resumed-cooperation-on-missiles-un-says; “UN Report Says Iran and North Korea Resumed Missile Cooperation,” Radio Free Europe / Radio Liberty, February 9, 2021, https://www.rferl.org/a/un-report-says-iran-and-north-korea-resumed-missile-cooperation/31093315.html; and “North Korea-Iran missile cooperation is reason for ambitious diplomacy,”

The Survival Editor's Blog, February 15, 2021, https://www.iiss.org/blogs/survival-blog/2021/02/north-korea-iran-missile-cooperation.

111 "North Korea hits back at the UNSC for calling its space program threatening," Business Insider India, November 20, 2020, https://www.businessinsider.in/science/space/news/north-korea-hits-back-at-the-unsc-for-calling-its-space-programs-threatening/articleshow/79319410.cms.

112 Yonhap, "NK pushing for five-year space development program purely for peaceful purposes: state media," *Korean Herald,* April 2, 2020, http://www.koreaherald.com/view.php?ud=20200402000655; and Colin Zwirko, "North Korean TV airs new segment promoting national space program," NK News, May 29, 2020, https://www.nknews.org/2020/05/north-korean-tv-airs-new-segment-promoting-national-space-program/.

113 Elizabeth Shim, "North Korea highlights space program in state media," UPI, April 2, 2020, https://www.upi.com/Top_News/World-News/2020/04/02/North-Korea-highlights-space-program-in-state-media/8821585835441/.

114 "Sohae Satellite Launching Station: Service Roads Regraded," 38 North, March 31, 2020, https://www.38north.org/2020/03/sohae033120/; Peter Makowsky and Jack Liu, "Sohae Satellite Launching Station: Signs of Daily Life," 38 North, December 4, 2020, https://www.38north.org/2020/12/sohae201204/; and Peter Makowsky and Jack Liu, "Sohae Satellite Launching Station: Snow Removal Underway," 38 North, February 5, 2021, https://www.38north.org/2021/02/sohae-satellite-launching-station-snow-removal-underway/.

115 "North Korean Direct Ascent Anti-Satellite Weapons," Weapons and Warfare, October 16, 2020, https://weaponsandwarfare.com/2020/10/16/north-korean-direct-ascent-anti-satellite-weapons/.

116 Colin Zwirko, "North Korean TV airs new segment promoting national space program," NK News, May 29, 2020, https://www.nknews.org/2020/05/north-korean-tv-airs-new-segment-promoting-national-space-program/.

117 "North Korean Direct Ascent Anti-Satellite Weapons," Weapons and Warfare.

118 David Axe, " Kim Jong Un Throws Down a Nuclear Gauntlet – His Regime will Build a Solid-Fuel ICBM," *Forbes,* January 14, 2021, https://www.forbes.com/sites/davidaxe/2021/01/14/kim-jong-un-throws-down-a-nuclear-gauntlet-his-regime-will-build-a-solid-fuel-icbm/?sh=29f6544b75b4.

119 "No Dong 1," Missile Threat, CSIS, June 15, 2018, https://missilethreat.csis.org/missile/no-dong/; and David Wright, Laura Grego, and Lisbeth Gronlund, The Physics of Space Security: A Reference Manual (Cambridge, MA: American Academy of Arts and Sciences, 2005), 77, https://aerospace.csis.org/wp-content/uploads/2019/06/physics-space-security.pdf.

120 "North Korean Direct Ascent Anti-Satellite Weapons," Weapons and Warfare, October 16, 2020, https://weaponsandwarfare.com/2020/10/16/north-korean-direct-ascent-anti-satellite-weapons/.

121 Peter Pry, "North Korea's Satellites Could Unleash Electromagnetic Pulse Attack," Center for Security Policy, March 11, 2019, https://www.centerforsecuritypolicy.org/2019/03/11/north-koreas-satellites-could-unleash-electromagnetic-pulse-attack/; Rajesh Uppal, "China, North Korea, and Others Developing Super-EMP and Other Electromagnetic Weapons, Posing Serious Threat to Civil Society," International Defense Security & Technology, August 31, 2020, https://idstch.com/geopolitics/the-rise-of-emp-and-microwave-weapons-or-weapons-of-mass-electrical-destruction-pose-threat-to-civil-society/; and Peter Pry, "EMP ignorance is bliss," Secure the Grid, August 5, 2020, https://securethegrid.com/2020/08/05/emp-ignorance-is-bliss/.

122 Jeong Tae Joo, "N Korea readies deployment of new GPS jamming device," Daily NK, April 27, 2020, https://www.dailynk.com/english/north-korea-readies-deployment-new-gps-jamming-device/; and "North Korea is Enhancing its Electronic Warfare Capabilities," iHLS, May 1, 2020, https://i-hls.com/archives/100960.

123 Steven Silver, "Is North Korea Jamming Radio Signals?," *National Interest,* January 7, 2021, https://nationalinterest.org/blog/korea-watch/north-korea-jamming-radio-signals-175977; Mun Dong Hui, "North Korea appears to be jamming Unification Media Group radio broadcasts," Daily NK, January 7, 2021, https://www.dailynk.com/english/north-korea-appears-jamming-unification-media-group-radio-broadcasts/; and "North Korean Direct Ascent Anti-Satellite Weapons," Weapons and Warfare, October 16, 2020, https://weaponsandwarfare.com/2020/10/16/north-korean-direct-ascent-anti-satellite-weapons/.

124 Department of the Army, North Korean Tactics, Army Technical Publication 7-100.2 (Washington, DC: July 2020), https://fas.org/irp/doddir/army/atp7-100-2.pdf.

125 Eduard Kovacs, "U.S. Army Report Describes North Korea's Cyber Warfare Capabilities," Security Week, August 18, 2020, https://www.securityweek.com/us-army-report-describes-north-koreas-cyber-warfare-capabilities; and Department of the Army, North Korean Tactics.

126 Kovacs, "U.S. Army Report Describes North Korea's Cyber Warfare Capabilities"; and Department of the Army, North Korean Tactics.

127 Yonhap, "Pompeo says N. Korea a greater threat than Russia in cyber security," *Korea Herald,* December 15, 2020, http://www.koreaherald.com/view.php?ud=20201215000110&np=13&mp=2.

128 "U.S. says threat posed by North Korea cyber activity part of policy review," Reuters, February 17, 2021, https://www.reuters.com/article/idUSKBN2AH2PA.

129 Eric Tucker, "US charges North Korean computer programmers in global hacks," Associated Press, February 17, 2021, https://apnews.com/article/us-charges-north-korea-global-hacks-3c8145431462830e8f80e1576f731577.

130 Ibid.

131 Edith Lederer, "UN experts: North Korea using cyberattacks to update nukes," Associated Press, February 9, 2021, https://apnews.com/article/technology-global-trade-nuclear-weapons-north-korea-coronavirus-pandemic-19f536cac4a84780f54a3279ef707b33.

132 Ibid.

INDIA

133 Paulo Shakarian, "North Korea targeted cybersecurity researchers with hacking, espionage," UPI, February 5, 2021, https://www.upi.com/Top_News/Voices/2021/02/05/North-Korea-targeted-cybersecurity-researchers-with-hacking-espionage/8221612529846/.

134 Ibid.

135 "About ISRO," ISRO, https://www.isro.gov.in/about-isro.

136 Hanneke Weitering, "India's Space Agency Breaks Dry Spell with Its 1st Rocket Launch of 2020," Space.com, November 10, 2020, https://www.space.com/india-pslv-rocket-1st-launch-2020.

137 Andrew Jones, "Indian PSLV rocket launches Brazilian Amazonia-1 satellite," *SpaceNews*, February 28, 2021, https://spacenews.com/indian-pslv-rocket-launches-brazilian-amazonia-1-satellite/.

138 Vivek Raghuvanshi, "India to Launch a Defense-Based Space Research Agency," *Defense News,* June 12, 2019, https://www.defensenews.com/space/2019/06/12/india-to-launch-a-defense-based-space-research-agency/.

139 John Sheldon, "Indian Space Wars: India's DRDO Head Outlines Counterspace Capability Ambitions," SpaceWatch.Global, April 15, 2019, https://spacewatch.global/2019/04/indian-space-wars-indias-drdo-head-outlines-counterspace-capability-ambitions/.

140 Aakriti Sharma, "India's Defense Space Agency Hunting for New Technology That Can Track Enemy Assets," EurAsian Times, February 24, 2021, https://eurasiantimes.com/india-steps-up-space-warfare-program-begins-hunt-for-new-technology.

141 Rajat Pandit "ASAT Missile: Satellite-Killer Not a One-off, India Working on Star Wars Armoury," *Times of India,* April 7, 2019, https://timesofindia.indiatimes.com/india/satellite-killer-not-a-one-off-india-working-on-star-wars-armoury/articleshow/68758674.cms.

142 "DRDO Accelerates Work on 'Laser Weapons'; But Where Does India Stand Against China, Russia, and The US?," EurAsian Times, September 28, 2020, https://eurasiantimes.com/drdo-accelerates-work-on-laser-weapons-but-where-does-india-stand-against-china-russia-the-us.

143 "Technologies," Defence Research and Development Organisation - DRDO, Ministry of Defence, Government of India, https://www.drdo.gov.in/labs-establishment/technologies/laser-science-technology-centre-lastec.

144 "Electronic Warfare – Denying Electromagnetic Advantage to Enemy," SP's Land Forces - Defence, http://www.spslandforces.com/story/?id=698.

145 "Himshakti EW:- India Indigenous Electronic Warfare System," Indian Defence News, May 4, 2019, https://defenceupdate.in/himshakti-ew-india-indigenous-electronic-warfare-system/.

146 Ibid.; and IANS, "Pakistan's Radars Were Jammed by IAF during Airstrike at Balakot," *Business Standard,* February 26, 2019, https://www.business-standard.com/article/news-ians/pakistan-s-radars-were-jammed-by-iaf-during-airstrike-at-balakot-119022601215_1.html.

147 "(Formerly NM Urban) Homesteader - Blog," https://formerlynmurbanhomesteader.weebly.com/uploads/2/2/5/0/22509786/weebly_formerlynmurbanhomesteader_links_master__version_1_autosaved_.xlsx.

148 John Leyden, "Indian Cyber-Espionage Activity Rising amid Growing Rivalry with China, Pakistan," Daily Swig, February 25, 2021, https://portswigger.net/daily-swig/indian-cyber-espionage-activity-rising-amid-growing-rivalry-with-china-pakistan.

OTHERS

149 Jim Garamone, "Chief of Space Operations Discusses Need for Outreach to Partners, State of Space Force," U.S. Department of Defense, November 25, 2020, https://www.defense.gov/Explore/News/Article/Article/2427918/chief-of-space-operations-discusses-need-for-outreach-to-partners-state-of-spac/.

150 AFP Staff Writers, "France conducts first military drills in space," Spacewar, March 9, 2021, https://www.spacewar.com/reports/France_conducts_first_military_drills_in_space_999.html.

151 SPIE Europe Ltd, "Israeli Ministry of Defense Claims Laser Weapon Breakthrough," Optics.org, accessed March 5, 2021, https://optics.org/news/11/1/25.

152 "Israel's Space-Age Laser Weapon Targets Explosive Balloons from Gaza," VOA, accessed March 5, 2021, https://www.voanews.com/episode/israels-space-age-laser-weapon-targets-explosive-balloons-gaza-4407646.

153 Joanne Wheeler ed., The Space Law Review, 2nd ed. (London: December 2020), https://thelawreviews.co.uk/title/the-space-law-review.

154 Doug Messier, “An Overview of Japan’s Counterspace Strategy,” Parabolic Arc, April 26, 2020, http://parabolicarc.com/2020/04/26/an-overview-of-japans-counterspace-strategy/.

155 Mari Yamaguchi, “Japan Launches New Unit to Boost Defense in Space,” *Defense News,* May 18, 2020, https://www.defensenews.com/global/asia-pacific/2020/05/18/japan-launches-new-unit-to-boost-defense-in-space/; “Japan’s New Space Domain Mission Unit and Security in the Indo-Pacific Region,” International Institute for Security Studies, accessed March 5, 2021, https://www.iiss.org/blogs/military-balance/2020/05/japan-space-domain-mission-unit-security; and Suzuki Kazuto, “Space: A New Battleground for Japan,” Nippon, December 5, 2018, https://www.nippon.com/en/in-depth/a06101/.

156 Sam Wilson, “Japan’s Gradual Shift Toward Space Security,” *The Diplomat,* May 6, 2020, https://thediplomat.com/2020/05/japans-gradual-shift-toward-space-security/; Yamaguchi, “Japan Launches New Unit to Boost Defense in Spacehttp://www.nids.mod.go.jp/english/research/profile/anzen/06-fukushima.html.

157 Doug Messier, “An Overview of Japan’s Counterspace Strategy,” Parabolic Arc, April 26, 2020, http://parabolicarc.com/2020/04/26/an-overview-of-japans-counterspace-strategy/.

158 Dana A. Goward et al., “South Korea Discusses Decision to Combine GPS and ELoran,” Geospatial World, November 17, 2020, https://www.geospatialworld.net/blogs/south-korea-discusses-decision-to-combine-gps-and-eloran/.

159 이원주, “Upcoming Military Exercise with U.S. Should Be Postponed or Halted: Expert,” Yonhap News Agency, February 25, 2021, https://en.yna.co.kr/view/AEN20210225009200325.

160 “Air Commodore Paul Godfrey announced as Commander United Kingdom Space Command,” Royal Air Force, February 1, 2021, https://www.raf.mod.uk/news/articles/air-commodore-paul-godfrey-announced-as-commander-united-kingdom-space-command/.

161 Steve Shaw, “Britain Gears Up To Join the Space Arms Race,” Byline Times, December 3, 2020, https://bylinetimes.com/2020/12/03/britain-gears-up-to-join-the-space-arms-race/.

WHAT TO WATCH

162 Chad J. R. Ohlandt, Bruce McClintock, and Stephen J. Flanagan, “Navigating Norms for the New Space Era,” National Interest, February 8, 2021, https://nationalinterest.org/feature/navigating-norms-new-space-era-177592.