MARCH 2020

A REPORT OF
THE CSIS
AEROSPACE
SECURITY
PROJECT

SPACE THREAT ASSESSMENT 2020

Principal Authors
TODD HARRISON
KAITLYN JOHNSON
THOMAS G. ROBERTS
TYLER WAY
MAKENA YOUNG

Foreword
MARTIN C. FAGA

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

MARCH 2020

SPACE THREAT ASSESSMENT 2020

Authors
TODD HARRISON
KAITLYN JOHNSON
THOMAS G. ROBERTS
TYLER WAY
MAKENA YOUNG

Foreword
MARTIN C. FAGA

A REPORT OF THE
CSIS AEROSPACE SECURITY PROJECT

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

ABOUT CSIS

For over 50 years, the Center for Strategic and International Studies (CSIS) has worked to develop solutions to the world's greatest policy challenges. Today, CSIS scholars are providing strategic insights and bipartisan policy solutions to help decisionmakers chart a course toward a better world.

CSIS is a nonprofit organization headquartered in Washington, D.C. The Center's 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look into the future and anticipate change.

Founded at the height of the Cold War by David M. Abshire and Admiral Arleigh Burke, CSIS was dedicated to finding ways to sustain American prominence and prosperity as a force for good in the world. Since 1962, CSIS has become one of the world's preeminent international institutions focused on defense and security; regional stability; and transnational challenges ranging from energy and climate to global health and economic integration.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in November 2015. Former U.S. deputy secretary of defense John J. Hamre has served as the Center's president and chief executive officer since 2000.

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

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. The authors would like to thank Martin C. Faga, Brian Weeden, Victoria Samson, Emily Tiemeyer, Jeeah Lee, and Jacque Schrag for their support of this project.

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

CONTENTS

FOREWORD

MUCH IS SAID THESE DAYS about the possibility of conflict in space during, before, or perhaps, instead of conflict on land, at sea, or in the air. Why is this the case?

The subject is discussed as though it emerged in the last 13 years since the Chinese demonstration of a kinetic ASAT in 2007. In fact, the United States was concerned in 1957 that Sputnik represented a precursor to space-based nuclear weapons. An ASAT program started in the United States in 1958, and the Soviets did similarly. Both superpowers deployed several ASAT systems and performed orbital tests.

Nonetheless, fear on both sides of a serious threat of conflict in space did not emerge until recently. Both the Soviets and the United States understood that the satellites of "National Technical Means" were stabilizing and were keys to de-escalation should a conflict occur. This view changed after the First Gulf War, when space systems moved from being primarily strategic systems to tactical ones providing near real-time support to tactical forces. By that time, the satellites of the Department of Defense and of the Intelligence Community operated and reported almost instantly, and the military services developed the equipment and techniques to acquire, analyze, and distribute space system information very quickly.

Following the First Gulf War, a Russian analysis of the rapid American success noted the efficacy of precision weapons and real-time intelligence. Much of this capability depended on space systems and spurred the Russians and Chinese to a sustained program to develop ASAT capabilities--not only those for physical attack but cyber and electronic attacks as well. In recent years, we have read Russian and Chinese doctrine explaining the importance of ASAT capabilities, and we have seen systems deployed to carry them out.

The situation we confront today was inevitable. Capability is always met with counter-capability. In recognition of this need to defend and to increase our space power in the face of such threats, the United States has wisely created the Space Force and the U.S. Space Command. This is where the people who will design, build, and operate our military space systems reside and where personnel will be trained, careers managed, doctrine developed, and a myriad other elements of a military force undertaken.

Several years ago, an Army general gave a speech where he said, "every company commander depends on space, and takes it for granted." What a challenge for our Space Force and Space Command to assure that our military is served at every level of command without failing.

MARTIN C. FAGA

Former Assistant Secretary of the Air Force for Space and Director of the National Reconnaissance Office

INTRODUCTION

THE PAST YEAR WAS A TRANSFORMATIONAL ONE for space policy in several respects. On December 20, 2019, President Trump signed into law the National Defense Authorization Act for Fiscal Year 2020, creating the Space Force and ushering in what is arguably the most significant reorganization of the U.S. military since the Goldwater Nichols Act of 1986. While the newly created Space Force is responsible for organizing, training, and equipping space forces for the U.S. military, the newly re-established United States Space Command is the geographic combatant command responsible for space operations.

France also made significant organizational changes in 2019 with the issuance of its Space Defense Strategy. It calls for the creation of a Space Command within the Air Force and the renaming of the Air Force to the Air and Space Force. The French defense minister publicly stated that France would develop space control capabilities and active defenses, such as small bodyguard satellites and space-based laser defenses to protect important space assets.

Other countries continue to develop and test counterspace capabilities and conduct suspicious or threatening activities in space. India became the fourth country to successfully test a direct-ascent anti-satellite (ASAT) missile, as well as the only country to conduct a debris-producing test since 2008. Russia continued its co-orbital activities in geostationary orbit (GEO) and caught the attention of many in the space community with its proximity operations around a classified U.S. government satellite in low Earth orbit (LEO).

In commercial space, both SpaceX and OneWeb began deployment of mega constellations in LEO to deliver high-speed internet access globally. OneWeb launched its first set of six satellites in February 2019, and SpaceX launched its first batch of 60 satellites in May 2019. Both companies have conducted additional launches since then, with SpaceX beginning to deploy at a steady pace in early 2020. As of February 17, 2020, SpaceX has launched a total of 302 Starlink satellites, 297 of which are operational. In comparison, the total number of operational satellites in LEO was roughly 1,500 in 2019—a number that could double by the end of 2020. These commercial developments present both opportunities and challenges in what is already a diverse, disruptive, disordered, and dangerous space environment.

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 focus more attention. While the report focuses on the capabilities of China, Russia, Iran, North Korea, and India, this year's report places relatively more emphasis than previous years on the counterspace capabilities of select other countries, including some allies and partners of the United States.

This report is not a comprehensive assessment of all foreign counterspace capabilities because much of the information on what other countries are doing is not publicly available. The information in this report is current as of February 22, 2020.

TYPES OF COUNTERSPACE WEAPONS

SPACE IS AN INCREASINGLY IMPORTANT ENABLER of economic and military power. The December 2017 United States National Security Strategy prioritizes maintaining U.S. leadership and freedom of action in this critical domain, but it notes that:

> *Many countries are purchasing satellites to support their own strategic military activities. Others believe that the ability to attack space assets offers an asymmetric advantage and as a result, are pursuing a range of anti-satellite (ASAT) weapons. The United States considers unfettered access to and freedom to operate in space to be a vital interest. Any harmful interference with or an attack upon critical components of our space architecture that directly affects this vital U.S. interest will be met with a deliberate response at a time, place, manner, and domain of our choosing.*[1]

Counterspace weapons vary in the types of effects they create, and the level of technological sophistication and resources required to develop and field them. They also differ in how they are employed and how difficult they are to detect and attribute. The effects of these weapons can be temporary or permanent, depending on the type of system and how it is used. The country-by-country assessments that follow this section group counterspace weapons into four broad categories: kinetic physical, non-kinetic physical, electronic, and cyber.

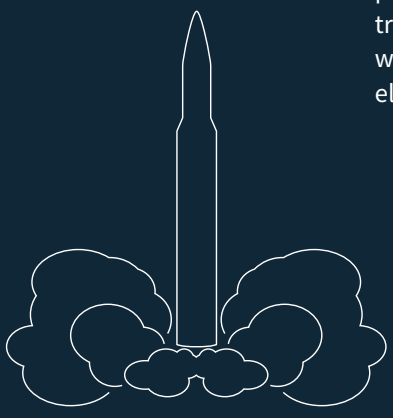


Illustration A ballistic missile can be used as a kinetic physical counterspace weapon.

KINETIC PHYSICAL

KINETIC PHYSICAL COUNTERSPACE weapons attempt to strike directly or detonate a warhead near a satellite or ground station. A direct-ascent ASAT weapon attempts to strike a satellite using a trajectory that intersects the target satellite without placing the interceptor into orbit. Ballistic missiles and missile defense interceptors can be modified to act as direct-ascent ASAT weapons provided they have sufficient energy to reach the target satellite's orbit. A co-orbital ASAT weapon differs from a direct-ascent weapon because it is first placed into orbit. When commanded, the satellite then maneuvers to strike its target. Co-orbital ASATs can remain dormant in orbit for days or even years before being activated. A key technology needed to make both direct-ascent and co-orbital ASAT weapons effective is the ability to detect, track, and guide the interceptor into a target satellite. An onboard guidance system requires a relatively high level of technological sophistication and significant resources to test and deploy.[2]

Ground stations are vulnerable to kinetic physical attacks by a variety of conventional military weapons, from guided missiles and rockets at longer ranges to small arms fire at shorter ranges. Because they are often highly visible, located outside of the United States, and are more accessible than objects in space, ground stations can be an easier target for adversaries seeking to disrupt or degrade space systems. Even if the ground stations themselves are difficult to attack directly, they can be disrupted indirectly by attacking the electrical power grid, water supply, and the high-capacity communications lines that support them.

Kinetic physical attacks generally have irreversible effects on the satellites and ground stations targeted. These counterspace weapons are likely to be attributable because the United States and others can identify the source of a direct-ascent ASAT launch or ground attack and can, in theory, trace a co-orbital ASAT's orbital data back to its initial deployment. In both cases, the attacker is likely to know whether its attack is successful almost immediately because the effects would be publicly visible through orbital debris or a damaged ground station.

NON-KINETIC PHYSICAL

NON-KINETIC COUNTERSPACE weapons, such as lasers, high-powered microwave (HPM) weapons, and electromagnetic pulse (EMP) weapons, can have physical effects on satellites and ground stations without making physical contact. 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.

High-powered lasers can be used to damage or degrade sensitive satellite components, such as solar arrays. Lasers can also be used to temporarily dazzle or permanently blind mission-critical sensors on satellites. Targeting a satellite from Earth with a laser requires high beam quality, adaptive optics, and advanced pointing control to steer the laser beam as it is transmitted through the atmosphere—technology that is costly and requires a high degree of sophistication.[3] 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. The attacker, however, will have limited ability to know if the attack was successful because it would not likely produce debris or other visible indicators.

An HPM weapon can be used to disrupt a satellite's electronics, corrupt data stored in memory, cause processors to restart, and, at higher

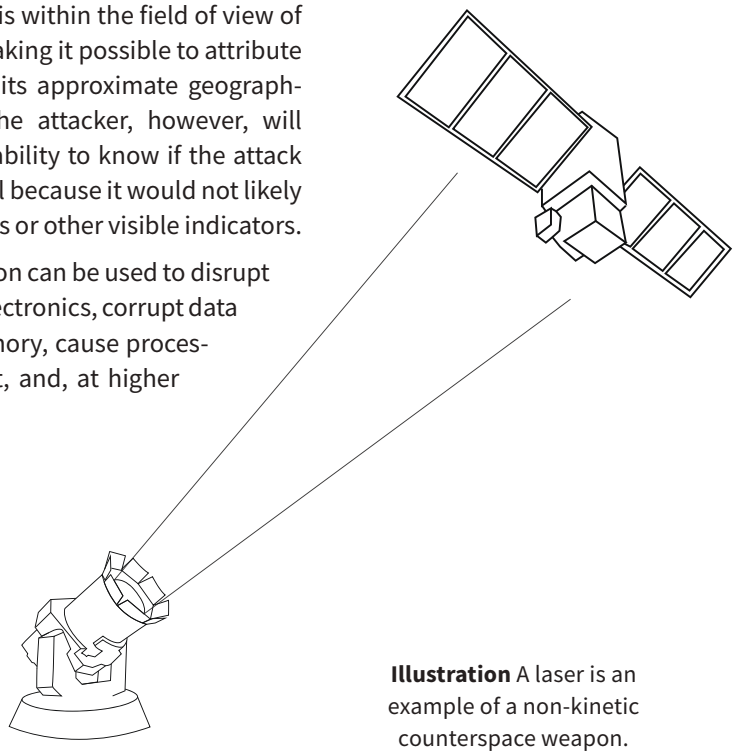


Illustration A laser is an example of a non-kinetic counterspace weapon.

power levels, cause permanent damage to electrical circuits and processors. A front-door HPM attack uses a satellite's own antennas as an entry path, while a backdoor HPM attack attempts to enter through small seams or gaps around electrical connections and shielding.[4] Because electromagnetic waves disperse and weaken over distance and the atmosphere can interfere with transmission at high power levels, an HPM attack against a satellite is best carried out from another satellite in a similar orbit. Both front-door and back-door HPM attacks can be difficult to attribute to an attacker, and as with a laser weapon, the attacker may not know if the attack has been successful.

The use of a nuclear weapon in space can be an indiscriminate form of non-kinetic physical attack. While a nuclear detonation would have immediate effects for satellites within range of its EMP, it also creates a high radiation environment that accelerates the degradation of satellite components over the long term for unshielded satellites in the affected orbital regime.[5]

ELECTRONIC

ELECTRONIC ATTACKS TARGET the means through which space systems transmit and receive data by jamming or spoofing radio frequency (RF) signals. Jamming is a form of electronic attack that interferes with RF communications by generating noise in the same frequency band and within the field of view of the antenna on the targeted satellite or receiver. An uplink jammer interferes with the signal going from the 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. 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 from a wider range of angles on the ground.[6]

The technology needed to jam many types of satellite signals is commercially available and relatively inexpensive. Jamming is a reversible form of attack because once a jammer is turned off, communications return to normal. Jamming can also be difficult to detect or distinguish from accidental interference, making attribution and awareness more difficult. In 2015, General John Hyten, then-commander of Air Force Space Command, noted that the U.S. military was unintentionally jamming its own communications satellites an average of 23 times per month.[7]

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. Spoofing the downlink from a satellite can be used to inject false or corrupted data into an adversary's communications systems. If an attacker successfully spoofs the command and control uplink signal to a satellite, it could take control of the satellite for nefarious purposes.

Through a type of spoofing called "meaconing," even the 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.[8] Like jammers, once a spoofer is developed, it is relatively inexpensive to produce and deploy in large numbers and can be proliferated to other state and non-state actors.

CYBER

UNLIKE ELECTRONIC ATTACKS, which interfere with the transmission of RF signals, cyberattacks target the data itself and the systems that use this data. The antennas on satellites and ground stations, the landlines that connect ground stations to terrestrial networks, and the

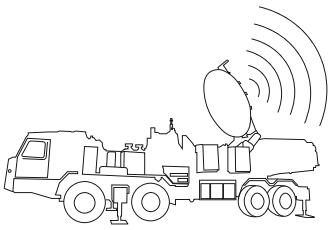


Illustration A truck-mounted jammer is a type of electronic counterspace weapon.

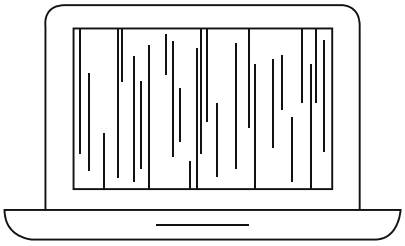


Illustration
Cyberattacks can be used to take control of a satellite and damage or destroy it.

user terminals that connect to satellites are all potential intrusion points for cyberattacks. Cyberattacks can be used to monitor data traffic patterns (i.e., which users are communicating), to monitor the data itself, or to insert false or corrupted data in the system. While cyberattacks require a high degree of understanding of the systems being targeted, they do not necessarily require significant resources to conduct. Cyberattacks can be contracted out to private groups or individuals, which means that a state or non-state actor that lacks internal cyber capabilities may still pose a cyber threat.[9]

A cyberattack on space systems can result in data loss, widespread disruptions, and even permanent loss of a satellite. For example, if an adversary can seize control of a satellite through a cyberattack on its command and control system, the attack could shut down all communications and permanently damage the satellite by expending its propellant supply or damaging its electronics and sensors. Accurate and timely attribution of a cyberattack can be difficult, if not impossible, because attackers can use a variety of methods to conceal their identity, such as using hijacked servers to launch an attack.

THREAT CHARACTERISTICS

The types of counterspace threats described above have distinctly different characteristics that make them more suitable for use in some scenarios than others. As shown in Table 1, some types of counterspace threats are difficult to attribute or have fully reversible effects, such as mobile jammers. High-powered lasers, for example, are “silent” and can carry out an attack with little public awareness that anything has happened. Other types of counterspace weapons produce effects that make it difficult for the attacker to know if the attack was successful, and some produce collateral damage that can affect space systems other than the one being targeted.

Counterspace weapons that are reversible, difficult to attribute, and have limited public awareness are ideally suited for situations in which an opponent may want to signal resolve, create uncertainty in the mind of its opponent, or achieve a fait accompli without triggering an escalatory response. For example, an adversary that wants to deter the United States from intervening in a situation may believe that such attacks will stay below the threshold for escalation (i.e., not trigger the very thing it is trying to prevent) while creating significant operational challenges for the United States that make the prospect of intervention more costly and protracted. Conversely, counterspace weapons that have limited battle damage assessment or that risk collateral damage may be less useful to adversaries in many situations. Without reliable battle damage assessment, for example, an adversary cannot plan operations with the confidence that its counterspace actions have been successful. Furthermore, weapons that produce collateral damage in space, such as large amounts of space debris, run the risk of escalating a conflict and turning other nations against the attacker.

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

Number of Successful Orbital Launches in 2019[10]

32

CHINA

"No force will stop or shake China or its people from achieving its goals"

PRESIDENT XI JINPING, 2019[11]

IN THE PAST DECADE, China has been barreling toward its lofty space goals. In the 2010s alone, China conducted over 200 successful orbital launches.[12] China's civil, military, and commercial capabilities are rapidly growing, and its 2020 plans show that the country aims to launch over 60 satellites into orbit via 40 launches over the coming year.[13]

China's civil space program is focused on its network of BeiDou positioning, navigation, and timing (PNT) satellites, similar to the U.S. Global Positioning System (GPS). China plans on launching two BeiDou satellites into geostationary orbit (GEO) in 2020 as well as further developing its Gaofen remote sensing satellite constellation. Since early 2019, *Chang'e-4*, the Chinese lunar lander mission that delivered a successful lunar rover called *Yutu-2*, has been conducting an exploration mission on the far side of the Moon. China plans to follow up this mission in late 2020 with *Chang'e-5*, a mission that aims to return samples from the Moon back to Earth for further study. To support its growing space capabilities, China has "built an expansive ground support infrastructure to support its growing on-orbit fleet and related functions including spacecraft and space launch vehicle (SLV) manufacture, launch, C2 [command and control], and data downlink."[14]

China also intends to send a mission to Mars with an orbiter and probe. This mission will include 13 science payloads and is on track for a July 2020 launch.[15] Three different launch vehicles are also scheduled to make their first flight in 2020: the Long March-5B, the Long March-7A, and the Long March-8.

The Long March-5B will be China's heavy-lift workhorse, supporting future exploration missions as well as the planned Chinese Space Station (CSS).[16] The first test launch of the -5B will likely take place in April 2020. If successful, it will be used to launch the first section of the modular CSS. The Long March-8 is planned to be China's first rocket with a reusable first stage and is planned to support China's growing commercial space sector.[17] Furthermore, "China aspires for a 2036 first human mission to the moon."[18]

China is continuing to move forward with a new modular space station. China has successfully operated two previous space labs in LEO, *Tiangong* 1 and *Tiangong* 2, through its Project 921 program, which began in 1992.[20] The new space station will consist of three modules. The core module of the CSS passed final review but is facing possible launch delays. Currently, it is expected to launch in 2020, while the two additional modules are planned for launch between 2022 and 2024.[21] Three or four manned missions and several cargo missions are also planned, but launch delays have caused schedules to slip for the entire program.[22] The station is estimated to have a 10-year lifespan, with the possibility of an extension.[23]

China is also expanding its international cooperation. China hosted a selection process for opportunities to host scientific payloads on the CSS. The final selection was announced in 2019 and includes nine projects, involving "23 institutions from 17 Member States of the United Nations in Asian-pacific, European, African, North American and South American regions."[24] China has furthered its space partnership with Russia through cooperating to develop "Russia's future *Luna-26* lunar orbiter, China's *Chang'e-7* lunar polar lander, and a joint lunar and deep space data center with a hub in each country."[25]

China's busiest launch site, the Xichang Satellite Launch Center, hosted 19 of China's 32 launches in 2019.[26] Located in the south of China, Xichang is currently expanding by adding another launch pad in order to keep pace with China's growing national and commercial launch demands.[27]

After a 2014 decree to allow private companies to develop SLVs, several new nominally private (though typically state-backed) Chinese companies began to develop and test new launch vehicles. China's commercial space companies grew from around 30 in 2017 to over 100 in 2018. This growth has led to the introduction of new commercial policies in 2019 in order to better regulate the growing commercial space launch sector.[29] These regulations have had a relatively positive response from Chinese commercial companies.[30]

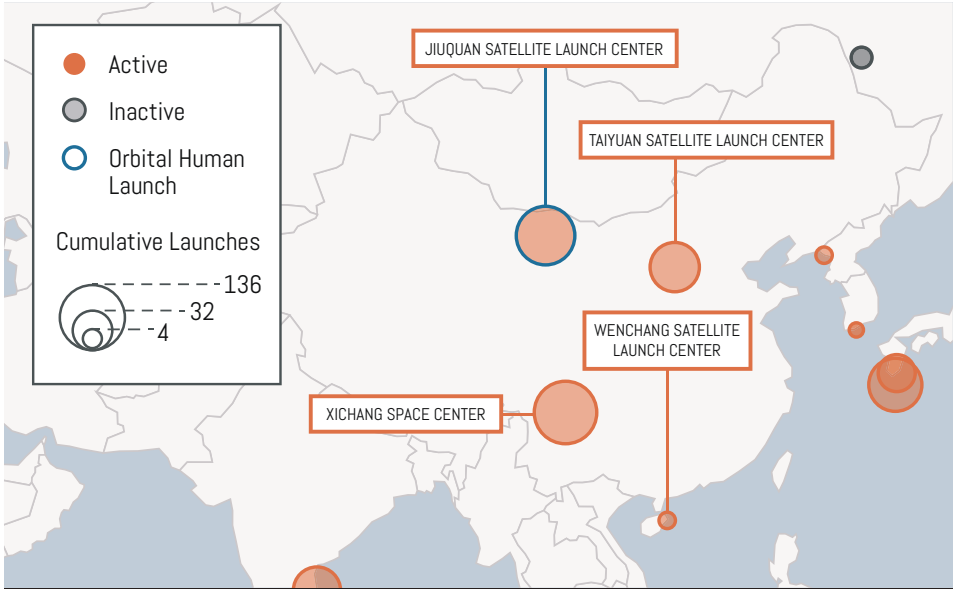


Figure 1: Chinese National Spaceports. China currently has four active spaceports, which have collectively launched hundreds of satellites and several taikonauts, or Chinese astronauts.

SPACE-TRACK.ORG / CSIS AEROSPACE SECURITY[28]

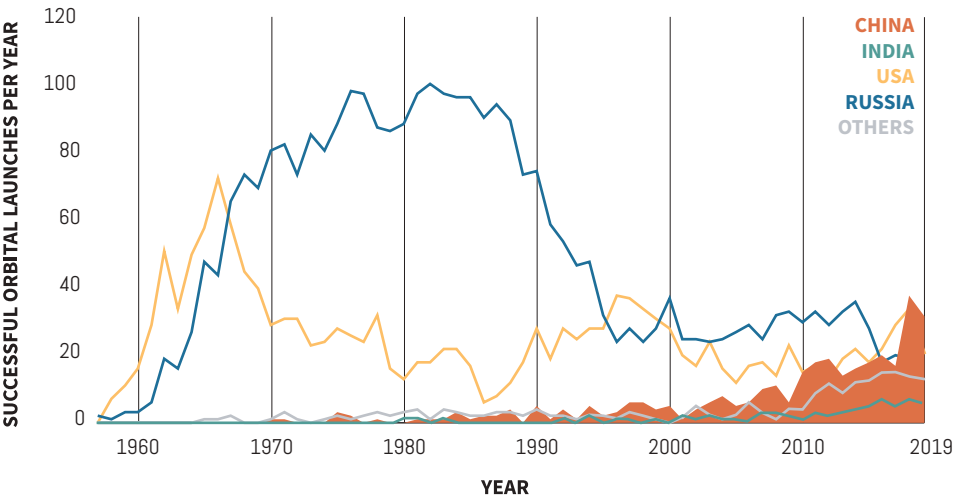


Figure 2: Chinese Orbital Space Launches (1957-2019). China had more successful orbital space launches in 2019 than any other nation.

SPACE-TRACK.ORG / CSIS AEROSPACE SECURITY[19]

SPACE ORGANIZATION AND DOCTRINE

The Chinese government operates separate civil and military space organizations. The China National Space Administration (CNSA) falls within the State Council's State Administration for Science, Technology, and Industry for National Defense (SASTIND) and is the primary organization for China's civil space activities. The main developer of national civil space technologies is the China Aerospace Science and Technology Corporation (CASC), a state-owned aerospace corporation. Meanwhile, military space activities are run through the People's Liberation Army (PLA). However, each of these entities collaborate with one another on developing space technologies.[31]

In July 2019, China released its first official defense white paper since 2015. Prior to this four-year gap, China had released similar white papers about every two years. Analysts acknowledge that the 2019 document "adds little to previous official reports on the details of recent reforms."[32] In line with how China views the space domain, the 2019 white paper references "outer space, electromagnetic space and cyberspace" all as one national defense aim.[33] China established the Strategic Support Force (SSF) in 2015 to bring the management of these strategic areas under one entity. Unlike the United States and even Russia, the PLA appears to view these three domains as inherently intertwined.

There is only one paragraph in the 2019 white paper that focuses solely on the space domain. It touts China's activity in international fora on space-related issues, such as the UN Office for Outer Space Affairs. The white paper recognizes space as of strategic importance to the nation and states that "space security provides strategic assurance for national and social development."[34] This rhetoric is consistent with other statements and posturing that China has demonstrated in recent years.

THE SSF HAS BEGUN TRAINING SPECIALIZED UNITS WITH DIRECT-ASCENT ASAT WEAPONS.

This also builds on the 2015 Chinese white paper, which stated that "outer space and cyberspace have become new commanding heights in strategic competition among all parties."[35] Many scholars interpreted this statement as a formal designation of both space and cyberspace as new warfighting domains.[36] To this end, the PLA founded the SSF to centralize and manage the military's space, cyber, and electronic warfare missions. Before the 2015 reorganization, responsibilities for cyber, space, and electronic warfare were scattered across at least four different PLA departments. The establishment of the SSF indicates the PLA's prioritization of these critical areas of warfare.[37]

In 2018, China published an Outline of Training and Evaluation doctrine, which emphasized joint warfare training between the different military services focused on combating "strong military opponents."[38] For the space domain, this is likely directed against the United States. Originally, the SSF was not assessed to have full control over China's ASAT capabilities. Experts believed that the responsibility for direct-ascent ASATs may lie with either the PLA's Rocket Force, which manages China's nuclear arsenal, or the PLA's Air Force.[39] However, recent records show that the SSF has begun training specialized units with direct-ascent ASAT weapons capable of targeting satellites in LEO.[40]

According to the U.S-China Economic and Security Review Commission, Beijing has "sought to leverage military-civil fusion to commercialize its existing space technology." Utilizing civil or commercial technologies to bolster or disguise its military space systems is a recognizable theme throughout China's counterspace weapons program. "The goal of military-civil fusion in China's space sector is not primarily to develop cutting-edge technology but to produce existing technology that meets most customers' needs at a lower cost and at greater commercial scale and efficiency."[41]

COUNTERSPACE WEAPONS

Kinetic Physical

China has very capable kinetic physical counterspace capabilities and has proven this several times with a range of direct-ascent ASAT weapons tests. Thus far, China's primary focus has been targets in LEO, but recent tests indicate China also has a direct-ascent capability able to reach GEO. It does not appear that China has successfully tested a co-orbital ASAT capability, although it has demonstrated several of the technical capabilities required to construct such a weapon.

"China continues development of multiple counterspace capabilities designed to degrade and deny adversary use of space-based assets during a crisis or conflict."

U.S. OFFICE OF THE SECRETARY OF DEFENSE [42]

China had its first successful test of a kinetic physical ASAT weapon in 2007, after two previous failed tests.[43] This test of a direct-ascent *SC-19* missile system targeted and destroyed an aging Chinese meteorological satellite, producing over 3,000 trackable pieces of debris in LEO. Around 2,800 trackable pieces of debris from this test remain in orbit, with 11 pieces deorbiting in 2019.[44] This debris threatens the safe operation of hundreds of other satellites in LEO, including the International Space Station (ISS).[45]

China has not conducted a debris-producing direct-ascent ASAT test since 2007. However, analysts believe several other kinetic physical tests—or suspected tests—have occurred since then.[46] These suspected tests have not to date produced orbital debris or threatened any orbiting satellite.[47] Table 2 summarizes several Chinese ASAT, or suspected ASAT, tests. The missile tests are harder to judge because they could also function as a counterspace capability during times of conflict.

China has also developed and launched several satellites which are testing technologies that could be used for co-orbital counterspace capabilities. None of these tests have resulted in a verifiable destructive incident. Primarily, China has been testing its rendezvous and proximity operations (RPO) capabilities, a dual-use technology used to maneuver satellites in orbit near one another. Whether this maneuvering is for nefarious purposes, possibly making it a co-orbital ASAT, or for peaceful purposes, such as for on-orbit servicing or active debris removal missions, is unclear. Distinguishing the intent of the RPO movements is critical to determining whether or not a satellite is

Table 2

DIRECT-ASCENT ASAT OR DUAL-USE TESTS

Type	Year	Weapons System	Comments	Kinetic Impact?
ASAT test	2005	*SC-19*	Failed intercept of target. First recorded test for a direct-ascent ASAT.	No.
ASAT test	2006	*SC-19*	Failed intercept of target.	No.
ASAT test	2007	*SC-19*	Successful intercept of target.	Yes, and created thousands of debris on-orbit.
Missile defense test (suborbital)[48]	2010	*SC-19*	Reported successful technology test against a suborbital target. Likely "an effort to understand the homing performance of the interceptor."[49]	Yes.
Missile defense test (suborbital)	2013	Possibly *SC-19*[50]	Reported successful technology test against a suborbital target. Likely another technology demonstration test.[51]	Yes.
ASAT test	2013	*DN-2*	China declared the test as a high-altitude science mission. U.S. military assessed the test as proof Chinese direct-ascent ASATs could reach targets up to GEO.[52]	No.
ASAT test	2014	*SC-19*[53]	China claimed it was a land-based missile interceptor test, while the United States assessed the test as a non-destructive ASAT test.[54]	No. Possibly done to test timing capabilities.[55]
ASAT test	2015	*DN-3*[56]	China claimed it was a land-based missile interceptor test, while the United States assessed the test as a non-destructive ASAT test.[57]	No.
Missile defense test	2017	*DN-3*	Unsuccessful test of the DN-3 missile interceptor.[58]	No.
Missile defense test	2018	*DN-3*	DN-3 midcourse interceptor successfully intercepted its DF-21 target.[59]	Yes.

a counterspace weapon, but determining intent is almost impossible until a hostile action takes place. According to the U.S.-China Economic and Security Review Commission, "China's testing of RPOs has been similar to past U.S. tests, and no country has criticized RPOs carried out by China as illegal or violating any norm." China, Russia, and the United States all have satellites in GEO performing RPO activities around other satellites in orbit.[60]

"China has engaged in dual-use activities such as rendezvous and proximity operations (RPO)—which demonstrate co-orbital capabilities—that, while not prohibited, create problems for U.S. national security."

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION[61]

China has been testing these technologies for over a decade. For example, in 2008, a Chinese spacecraft deployed a miniature imaging satellite, the *BX-1*, that was jettisoned from its mother spacecraft. It appears that the satellite was unable to be actively controlled until after it had passed the International Space Station. It is estimated that the uncontrolled satellite came within 25 kilometers of the station. Despite many reports in the United States claiming that this was the first co-orbital ASAT test from China, the maneuver appears to have been unintentional.[62]

SJ-12, a Chinese satellite in LEO, conducted a series of remote proximity maneuvers with an older Chinese satellite, *SJ-06F*, in 2010. The maneuvers appeared to be slow, methodical, and intentional and occurred over several weeks in the summer of 2010.[63] Some have speculated that this mission was designed to test co-orbital jamming or other counterspace capabilities, however this has not been definitively proven in an unclassified setting.[64] At one point, *SJ-12* made contact with *SJ-06F* at low speed; however, this incident was "unlikely to have resulted in debris or significant damage to either satellite."[65] Testing RPO capabilities may have been a test run for the 2011 docking of the Shenzhou space capsule with the *Tiangong-1* space station, but the *SJ-12* maneuver could have serious counterspace implications as well.[66]

China has also been testing satellites with robotic arms, a dual-use technology that could be used as a test bed for docking operations for China's future space station, active debris removal missions, or a co-orbital ASAT. In 2013, China claimed that three new satellites were "conducting scientific experiments on space maintenance technologies."[67] However, U.S. officials reported that the one satellite was equipped with a robotic arm, which tested its ability to grapple and seize another satellite.[68]

Three years later, in 2016, China launched the *Aolong-1* spacecraft, which included a robotic arm and a sub-satellite that would be released and recovered during its mission. According to official statements, the *Aolong-1* was intended to test technologies needed to collect and deorbit space debris. Experts have debated the success of this test.[69]

The South China Morning Post reported in 2019 about recently declassified government documents which showcased how decade-old Chinese satellite technology has provided a base for "the development of new weapon systems powered by artificial intelligence." It is unclear how AI is utilized, but the article reports that the new small satellites can be equipped with robotic arms for active debris-removal missions. This technology is, of course, dual-use and could theoretically be used on a range of objects in orbit. The declassified document states that China has been developing and testing this technology since 2008. Without elaborating further, the document claims that the robotic arm technology has also been incorporated into "drones, smart weapons and robots." The article also claims that these satellites could remain attached to the debris it collects "to avoid being tracked from the ground."[70]

On the same mission as *Aolong-1*, China also deployed the *Tianyuan-1* spacecraft, which according to Chinese press accounts successfully tested the ability to refuel other satellites while in orbit.[71] This test, as well as the Aolong-1 test, received significant media coverage in the United States due to its potential dual-use as ASAT weapons.

While none of China's RPO activities in LEO or GEO appear to have damaged other satellites, these technological advancements in RPO have many experts concerned about China's intent. And unlike Russian RPO activity, China's RPO activities have been primarily focused on other Chinese satellites.

China can also pose a threat to space systems through its ability to attack the ground stations that control satellites

Taking a Break, SJ-17's Lack of Movement

***SJ-17*, A CHINESE SATELLITE** in geostationary orbit known for its unusual behavior, appears to have put a pause on its rendezvous and proximity operations in 2019. Compared to its first two years of operation, when the satellite appears to have performed close approaches and rendezvous operations with four Chinese satellites—*Chinasats 5A, 6A, 20,* and *1C*—the lack of movement in 2019 is notable. According to CSIS analysis, *SJ-17* restarted RPO maneuvers with another Chinese satellite in GEO, *Chinasat 6B*, in late December 2019 and was still in an unusually close orbit in late January 2020. In the past, *SJ-17*'s RPOs have lasted anywhere from a few weeks to over three months.[72] New analysis of *SJ-17*'s on-orbit activity also found that the satellite spent significant time near an Indonesian communications satellite, *Telkom 3S,* in late 2017 and early 2018, but there has been no public statement from Indonesia on *SJ-17*'s maneuvering within 10km of its satellite. In a 2015 paper published in a Chinese research journal, scientists speculated that a small satellite could be used to approach a large satellite in GEO in order to take high-quality pictures and quickly retreat or pass the target satellite to minimize detection.[73] While *SJ-17* is by no means a small satellite, it is possible that China is developing the skills and technology to accomplish such intelligence-gathering missions.[74]

with its conventional forces. China has the largest standing army of any nation, and over the past decade it has significantly increased its military budget and modernized its conventional military forces.[75] In a conflict, China could be capable of striking an adversary's satellite ground stations with ballistic missiles, cruise missiles, or long-range strike aircraft. As China's military reach continues to expand, it will be able to use its conventional forces to hold ground stations at risk over progressively greater distances.

Non-Kinetic Physical

In 2018, then-U.S. Director of National Intelligence Dan Coats assessed that China is making advances in directed-energy technology that can "blind or damage sensitive space-based optical sensors, such as those used for remote sensing or missile defense."[77] While this may sound like a major announcement of Chinese capabilities, China had already demonstrated its ability to dazzle American satellites in the mid-2000s. In 2006, reports surfaced that U.S. imaging satellites were illuminated by lasers over Chinese territory.[78] Then-Director of the National Reconnaissance Office (NRO) Donald Kerr acknowledged that U.S. imagery satellites were dazzled while passing over China but stated that it did not "damage the U.S. satellite's ability to collect information."[79] This incident demonstrates that China had much of the technology necessary to field an operational capability to dazzle

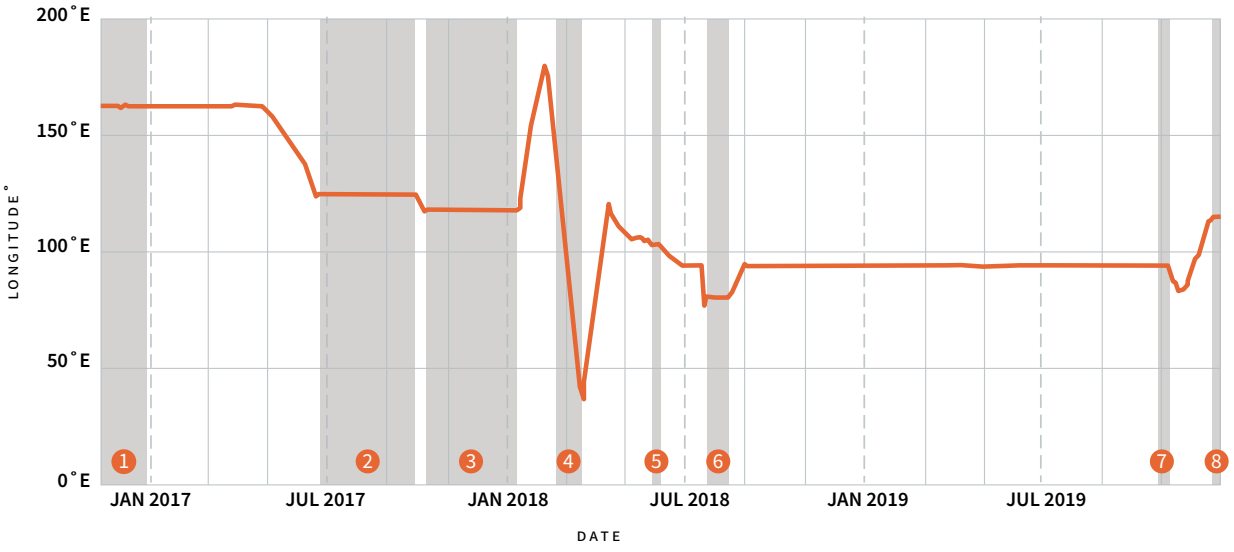
> "The [People's Liberation Army] is also deploying directed-energy weapons, and we expect them to field a ground-based laser system aimed at low-orbit space sensors by next year."
>
> THEN-ACTING SECRETARY OF DEFENSE PATRICK SHANAHAN[76]

Figure 3: 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 (2016-2019)

1. **Chinasat 5A** (China)
2. **Chinasat 6A** (China)
3. **Telkom 3S** (Indonesia)
4. **Chinasat 20** (China)
5. **Chinasat 2C** (China)
6. **Chinasat 1C** (China)
7. **Ekran 4** (Russia)
8. **Chinasat 6B** (China)



or blind a satellite back in 2006.[80] Recent statements indicate that China has continued to build and field more capable directed-energy systems. As one China expert highlighted, "the only fundamental barrier to learning these abstract elements [directed-energy] and achieving a practical weapon capability is effort—time, will, and money."[81]

Recently appointed Chief of Space Operations, General John J. Raymond noted in public remarks that, "we're pretty comfortable [in asserting] that they are developing directed energy weapons — probably building lasers to blind our satellites."[82] In early 2019, the Defense Intelligence Agency made a similar claim, stating "China likely is pursuing laser weapons to disrupt, degrade, or damage satellites and their sensors and possibly already has a limited capability to employ laser systems against satellite sensors."[83]

Chinese military and technical writings have often referenced directed-energy weapons as a key technology in a successful counterspace strategy.[84] The SSF is comprised of both Chinese space forces and electronic warfare-focused forces, likely indicating that the PLA sees interoperability between these two areas of warfare. Expert Mark Stokes testified that "The PLASSF Network Systems Department is central to China's counterspace mission." Stokes went on to explain that "Technical articles published . . . suggest the unit, at least in part, is responsible overseeing research, development, and acquisition of electronic counterspace systems." These same units may also be responsible for research and development and testing of high-powered microwave systems.[85]

In 2019, China surprisingly released an announcement alongside images of a new directed-energy system. This Chinese laser gun is reportedly designed to focus on small boats or drones.[86] While not directly a counterspace weapon, some of the technology would likely be similar for a higher-powered system that could affect a satellite in orbit. Furthermore, a top Chinese weapons firm is developing synthetic diamonds, also likely for use in directed-energy weapons. Diamonds can amplify and focus energy outputs to better ensure that the energy beam is intense enough to damage targets.[87]

Satellite imagery analysts speculated in early 2019 that China had been developing significant satellite lasing facilities.[88] Analysts speculate that China is pursuing these efforts in at least five different locations across the country, due to the nature of the buildings and surrounding infrastructure. One image even depicts a suspected electro-magnetic pulse (EMP) simulator suspended between two structures.[89] However, no other analysts appear to have corroborated these assessments.

China also announced an airborne laser in early 2020. While the details were confidential, the titles of two defense procurement bid requests may give insight on the PLA's plans. The two bids request the "procurement plan for airborne laser attack pod" and a "price inquiry on procurement plan for controlling software module of laser attack platform." The system appears to be intended to target other aircraft or missiles, but similar technology could be used to target satellites.[90]

While details from the PLA have been minimal and no public test has occurred on orbit, China has also shown interest in developing HPM weapons for air and missile defense. In January 2017, Chinese media celebrated the work of expert Huang Wenhua, who developed a miniaturized HPM weapon capable of being placed on a ship.[91] However, adding a mobile HPM system to a satellite would require further reductions in size, weight, and power in addition to a number of other integration challenges unique to the space environment.

As a nuclear power with intercontinental ballistic missiles (ICBMs), China also has the latent capability to launch a nuclear weapon into LEO. The resulting EMP from the detonation would cause indiscrimi-

CHINA IS LIKELY ALREADY DEVELOPING LASER WEAPONS AS PART OF ITS COUNTERSPACE STRATEGY.

nate damage to satellites, creating a high level of radiation in LEO that could last for years.[92] While China has the technology necessary to field a nuclear-armed ASAT weapon, it appears to be focusing its efforts in other areas.

Electronic

In the late-1990s, China acquired foreign ground-based satellite jamming equipment from Ukraine and has continued to develop the technology independently in the ensuing decades.[94] Currently, China has the ability to jam common satellite communication bands and GPS signals, and it has made the development and deployment of satellite jamming systems a high priority.[95] China is further developing jamming systems that will be able to target a large range of frequencies of commercial SATCOM as well as U.S. military protected communication bands.[96]

"The PLA considers EW [electronic warfare] capabilities key assets for modern warfare and its doctrine emphasizes using EW weapons to suppress or deceive enemy equipment."

DEFENSE INTELLIGENCE AGENCY, CHALLENGES TO SECURITY IN SPACE[93]

Chinese technical writings have been outspoken on how electronic warfare may increase its advantage in a conflict with the United States. A paper from the China Electronic Technology Group Corporation proposed solutions for "overcoming the high-power requirements for jamming U.S. millimeter wave (MMW) satellite communications by using space-based jammers hosted on small satellites, in a 'David versus Goliath' attack." The authors further identified U.S. satellites that would be particularly susceptible to such an attack, like "the Advanced Extremely High Frequency (AEHF), Wideband Global SATCOM (WGS), and Global Broadcast Service (GBS) satellite constellations."[97] Another Chinese technical paper provides further insight into how China plans to jam GPS signals used by U.S. drones, such as the RQ-4 Global Hawk, over the Spratly Islands and South China Sea.[98]

After the early 2020 U.S. drone strike on the Iranian general Qasem Soleimani, a Chinese military analyst commented that China would be able to detect an incoming strike through its early warning radars and anti-access/area denial (A2/AD) systems. He went on to say that China would be able to shoot down the drone with its air defenses and, as an added layer of defense, could conduct a "soft kill" by jamming the drone's communications and GPS.[99]

China has deployed military-grade truck-mounted jamming equipment in its buildup of military installations in the man-made islands in the South China Sea. As of April 2018, U.S. officials confirmed that there are two islands in the Spratly Island chain that have been equipped with jamming systems for targeting communications and radar. This assessment was supported by satellite imagery that shows a suspected jamming system on Mischief Reef in the Spratly Islands. While China has been building military installations across the island chain since 2014, this is the first visual evidence of jamming equipment there.[100] Shortly after the identification of the jammers, Vietnam condemned China's continued militarization and weaponization of the South China Sea and the Spratly Islands, also stating that the jamming equipment violates international law.[101]

In 2018, the SSF even carried out advanced military exercises simulating a complex electronic warfare environment with the "SSF base pitted against five PLA Army, Air Force, and Rocket Force units."[102]

China also reportedly developed a J-16D aircraft equipped with jamming systems. This aircraft, which suspiciously looks like the U.S. Navy's EA-18G Growler electronic attack fighter, is equipped with "several new antennas and conformal electronic-warfare arrays along the fuselage." According to the *National Interest*, the "D" in J-16D comes from *"diànzǐ,"* the Chinese word for electronic.[103]

Spoofing in the Port of Shanghai

INCIDENTS WERE REPORTED SPORADICALLY THROUGHOUT 2018 and 2019 of the GPS signals for Automatic Identification System (AIS) transponders being inaccurate in the main port of Shanghai. AIS signals broadcast the location, speed, and direction of a ship, as required by international maritime law.[104] Documented by a U.S. container ship, the *Manukai,* spoofing activities caused nearby ships' signals to be misrepresented in ways that could have caused a serious disaster. For example, a nearby docked ship's signal was reported as traveling down the channel toward the *Manukai* at significant speed. However, the captain of the *Manukai* could visually identify the ship in question as clearly docked and unmoving in a nearby slot at port. The incident did not stop there throughout the day, while the *Manukai* was securely docked at port, its AIS signals were reporting the ship being over three miles away from its actual location. The *Manukai* reported the incident to the U.S. Coast Guard which determined that there were "no known anomalies that might affect GPS signal integrity at the time and vicinity of the reported problem."[105]

Stunning for researchers is the peculiar circular shape of the plot of the spoofed ships and other GPS receivers in the area. Dubbed "crop circles" by confused researchers, this shape is unusual for GPS spoofing. According to Todd Humphries, a leading authority

on GPS jamming and spoofing, of the Radionavigation Laboratory at the University of Texas, Austin, declared "To be able to spoof multiple ships simultaneously into a circle is extraordinary technology." It is extraordinary because a single attack appears to have been able to spoof several vessels simultaneously, each to a different inaccurate location.[106] Furthermore, the D.C.-based research organization C4ADS also confirmed that civilian GPS was affected.

While the source of the spoofing remains unconfirmed, one expert traced the epicenter of the crop circle pattern to a non-operational smokestack near the port and speculates that it could be the origin of these GPS attacks.[107] GPS jamming and spoofing requires a direct line of sight to the target receiver. Therefore, to maximize impact and distance, many jamming devices are mounted on something with great height. For example, most military-grade truck-mounted jammers are mounted on a tall radio tower that maximizes the range of the effects.

Who is responsible? Again, this remains unclear. Early sources speculated that the attacks are actually GPS hacking caused by a non-state actor: sand smugglers.[108] However, the technology appears to be quite advanced, which researchers believe indicates that the Chinese government may be behind these attacks.

Another analyst, Bjorn Bergman, was intrigued by the reports and found similar crop circle phenomena in at least 20 other locations along the Chinese coast. Bergman assessed that 16 of these identified sites were oil terminals. A few of the other sites were Chinese government installations. Bergman assed that the oil terminals suggest that this could be an effort by the Chinese government to support Iran through importing Iranian crude oil in violation of sanctions.[109]

Due to the proximity to oil terminals, Bergman similarly assesses that the spoofing signals are being broadcast by the Chinese government.[110] Similarly, Humphries believes it is unlikely that a non-state actor could have developed this highly advanced technology.[111]

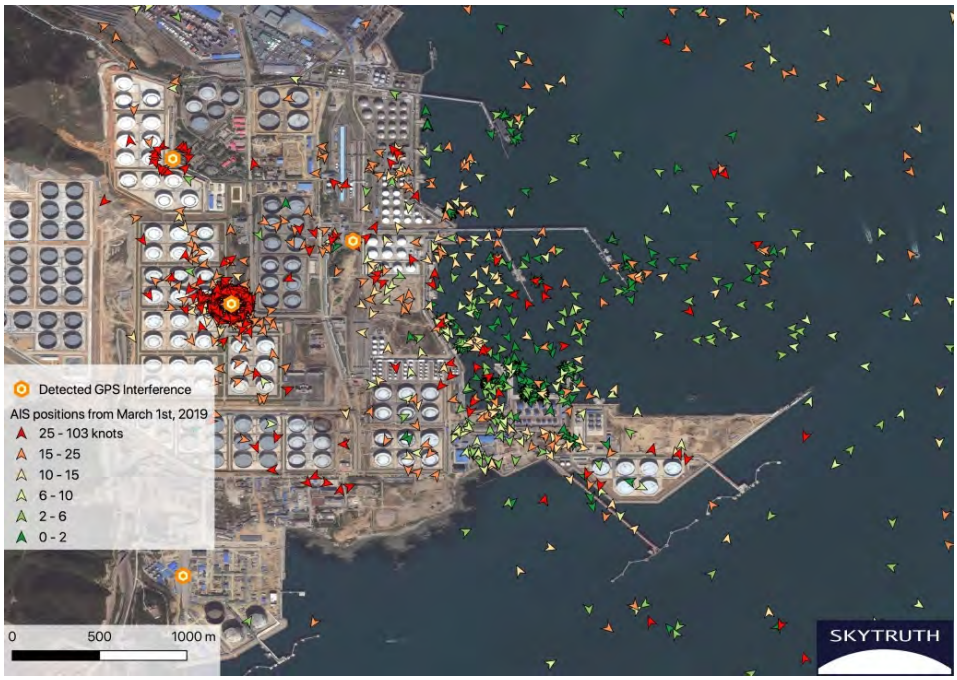
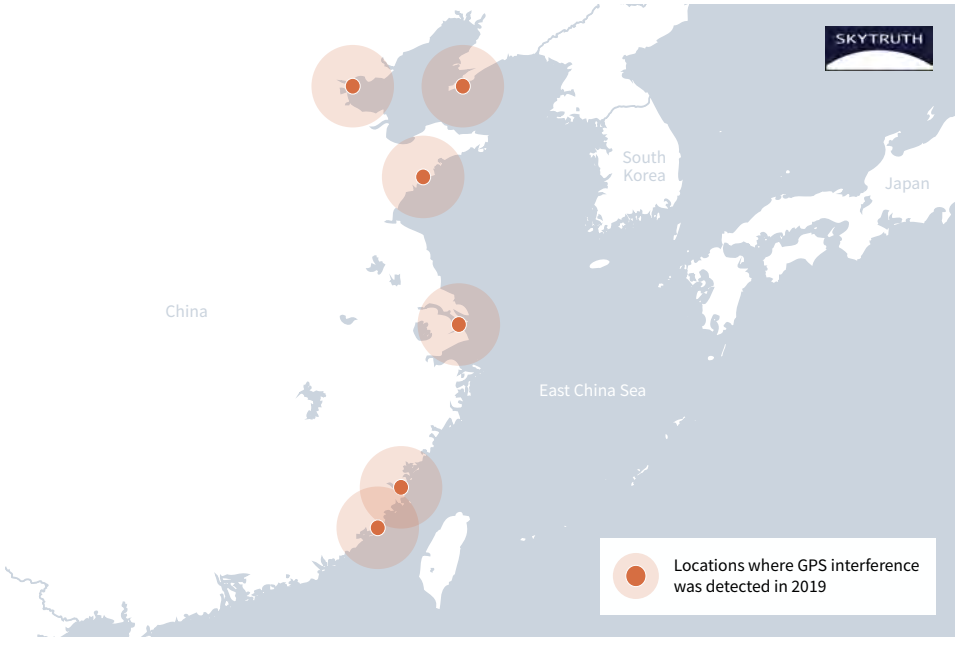


Figure 4 (above): GPS Crop Circles Near Dalian China. Research organization Skytruth found that two GPS interference locations around an oil terminal were active and had a dramatic effect on scrambling vessel positions in the area on September 5, 2019. Some vessels were even shown to be far inland. "On the water many positions are appearing with very high speeds (over 25 knots, red) and it's not possible to distinguish true and false locations. However, some slow speed positions (green) are appearing at dock where they would be expected, so some AIS broadcasts appear to be unaffected."

SKYTRUTH / AIS DATA COURTESY OF GLOBAL FISHING WATCH / ORBCOMM / SPIRE.

Figure 5 (below): Map of Reported AIS Outages Depicting the Crop Circle Patterns.

SKYTRUTH / AIS DATA COURTESY OF GLOBAL FISHING WATCH / ORBCOMM / SPIRE



"The PLA unit responsible for conducting signals intelligence has supported cyberespionage against U.S. and European satellite and aerospace industries since at least 2007."

DEFENSE INTELLIGENCE AGENCY, CHALLENGES TO SECURITY IN SPACE[112]

Cyber

Through the SSF, China has been integrating its advanced cyber capabilities with its counterspace and electronic warfare operations. The U.S. Defense Intelligence Agency assessed that: "The PLA could employ its cyberattack capabilities to establish information dominance in the early stages of a conflict to constrain an adversary's actions, or slow its mobilization and deployment by targeting network-based command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR), logistics, and commercial activities."[113]

Chinese hacks against secure government networks to steal personal information and technical data are well known, but the country's efforts to attack and infiltrate space systems has received relatively less attention.[114] Chinese writings and research efforts indicate that in a conflict it would attempt to conduct cyberattacks against U.S. satellites and ground stations.[115] Specifically, "PLA military writings detail the effectiveness of information operations and cyberwarfare in modern conflicts, and advocate targeting an adversary's Command and Control and logistics networks to affect the adversary's ability to operate during the early stages of conflict."[116]

China has already been implicated or suspected in several cyberattacks against U.S. satellites.[117] In October 2007 and again in July 2008, cyberattacks believed to originate in China targeted a remote sensing satellite operated by the U.S. Geological Survey called *Landsat-7*. These attacks are believed to have occurred through a ground station in Norway.[118] Each attack caused 12 or more minutes of interference with ground station communications, but the attackers did not gain control of the satellite. In June and October of 2008, hackers also believed to be from China attacked the National Aeronautics and Space Administration's (NASA) Terra Earth observation satellite. In these attacks, the hackers "achieved all steps required to command the satellite but did not issue commands."[119]

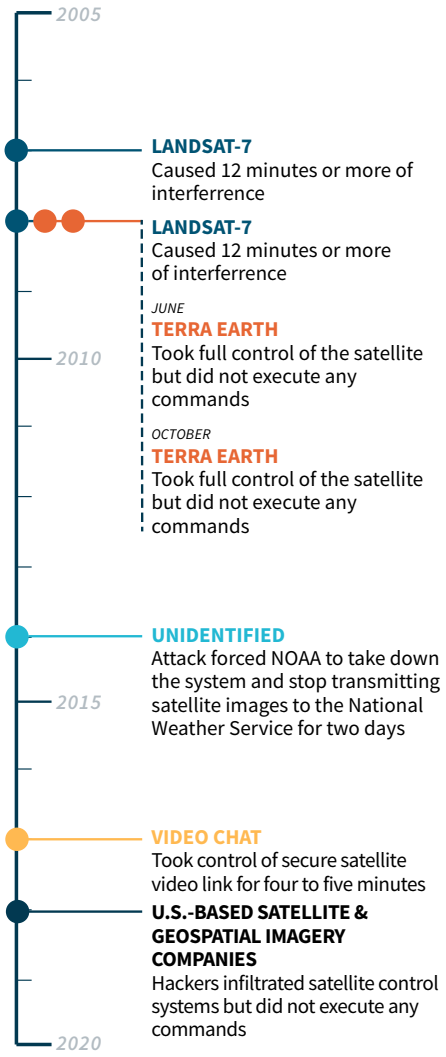


Figure 6: Timeline of Suspected Chinese Cyber Interference with Space Systems.

VARIOUS SOURCES COMPILED BY THE AEROSPACE SECURITY PROJECT

A 2019 NASA Inspector General report references several Chinese cyber intrusions into NASA, including a 2009 Chinese cyberattack on the Joint Propulsion Laboratory (JPL) which resulted in 22 gigabytes of data being transferred to a Chinese IP address. Another transfer of data to Chinese IP addresses occured in 2011 when "intruders gained full access to 18 servers supporting key JPL missions, including the DSN [Deep Space Network] and Advanced Spaceborne Thermal Emission and Reflection Radiometer mission, and

sensitive user accounts." The Advanced Spaceborne Thermal Emission and Reflection Radiometer mission is a joint project between NASA and Japan's Ministry of Economy, Trade, and Industry.[120]

In September 2014, Chinese hackers attacked National Oceanographic and Atmospheric Administration's (NOAA) satellite information and weather systems. The attack forced NOAA to take down the system and stop transmitting satellite images to the National Weather Service for two days before the organization was able to seal off the vital data.[121] After the attack was made public almost two months later, U.S. Representative Frank Wolf (R-VA) announced that NOAA had informed him that China was responsible for the hack on its systems. Chinese officials denied these claims, asserting that cyberattacks are common in today's world.[122]

Anonymous sources in India leaked in October 2017 that a "high-profile government meeting last month involving video chat via satellite was compromised by Chinese hackers". The video was in Chinese control for four to five minutes before Indian cybersecurity teams were able to launch a counterattack and neutralize the breach. The sources also claimed that the attack was able to breach the nation's "most sophisticated and secret link." However, the sources note that the Indian response team was unable to conclusively identify if the attack came from the Chinese government or non-state cybercriminals.[123]

On June 19, 2018, several researchers at Symantec—a U.S. software company—reported that a "sophisticated hacking campaign launched from computers in China burrowed deeply into satellite operators, defense contractors and telecommunications companies." The two targeted companies were U.S.-based satellite companies, a DoD submarine contractor, and a U.S. geospatial imaging company.[124] The researchers could not determine exactly which systems had been accessed in the breach, but they did admit that "the hackers infected computers that controlled the satellites, so that they could have changed the positions of the orbiting devices and disrupted data traffic." While Symantec did not directly blame the Chinese government for the attack, the company made it clear that the well-coordinated attack originated from the Chinese mainland.[125]

Later in 2018, the United States charged two Chinese nationals for their involvement in a decade-long cyber theft program, sponsored by the Chinese government. The program targeted aerospace industry companies, as well as NASA's Goddard Center and JPL. However, specific details of attacks by this group remain classified.[126]

SUMMARY

Overall, there appears to be an interesting shift in Chinese counterspace developments in 2019. Through the open-source assessment above, it appears that China has paused, or at least slowed, development and testing of its kinetic physical counterspace capabilities. This could be because its kinetic ASAT capabilities are well developed or because kinetic physical counterspace weapons are overt weapons that would likely draw a strong international condemnation if ever used. However, beginning in late December 2019 and through early January 2020, there is evidence that China's inspector satellite, *SJ-17*, was moving around in GEO, possibly signaling a return to operations after a hiatus of nearly a year.[127]

China is greatly increasing its development, testing, and fielding of non-kinetic physical and electronic counterspace weapons. The operational deployment of lasers capable of dazzling or blinding U.S. satellites seems imminent, if it has not occurred already. Furthermore, China is growing bolder with its electronic jamming and spoofing capabilities and may be using these technologies to hide illegal activities on its own coast or in the South China Sea. In 2020, it is likely that satellite jamming and spoofing capabilities will continue to be deployed and used in areas of gray zone conflict, such as the South China Sea and perhaps even to deter protests in Hong Kong.

China's cyberattacks against space systems have either not been publicly discussed or did not occur in 2019. However, this does not mean China is incapable of using cyber means to attack vulnerable space systems or has abandoned this line of effort.

Number of Successful Orbital Launches in 2019[128]

25

RUSSIA

"[Russian] leadership must be restored [in the space domain]. This is not just a question of prestige, but of national security."

DMITRY MEDVEDEV, FORMER RUSSIAN PRIME MINISTER[129]

WITH THE DISSOLUTION OF THE SOVIET UNION IN 1991, Russia inherited both the majority of the former state's vast space infrastructure and its place among the global space powers.[130] Since then, Russia has maintained a leading role in the global space community by operating the third-largest number of satellites on orbit, serving as a critical partner in international human spaceflight, and managing several of the world's busiest spaceports—all while facing an inconsistent federal budgetary environment and claims of widespread internal corruption.[131] By some metrics, Russia's space activity pales in comparison to the Soviet Union, which launched more payloads to orbit than all other countries combined before its collapse.[132] Other measurements, however, such as launch vehicle reliability and human spaceflight achievements, describe a formidable space actor with remarkable resilience in a rapidly changing space domain.

As the only ISS partner agency with a human-rated launch vehicle, Russia is responsible for ferrying all astronauts to and from the space station using its Soyuz rocket.[133] Since the U.S. Space Shuttle's final flight in 2011, Russia has launched 53 foreign astronauts to the ISS, including 34 Americans.[134] At over $80 million per seat, carrying passengers to orbit makes up 17 percent of the Russian space agency's annual budget, according to leaked budget documents from 2018.[135] For decades, NASA has had plans to develop a U.S. launch vehicle capable of transporting its astronauts to the ISS, lowering its dependence on the Russian Soyuz launch vehicle. With the first crewed flight test of the SpaceX Dragon capsule expected later this year as part of the U.S. Commercial Crew Program, the Russian space agency may soon find itself with many fewer human spaceflight customers compared to the past decade.[136]

RUSSIA

Despite the geopolitical tensions on Earth, Russia has pursued robust international partnerships in the space domain in addition to its commitments as part of the ISS agreement. For example, the Russian space agency has entered into discussions with the China National Space Administration to pursue cooperative lunar exploration missions beginning in 2020.[137] Since 2011, Russia has used the low-latitude Guiana Space Centre operated by the European Space Agency to launch Soyuz rockets, making it the only country in the world to launch a native orbital launch vehicle from a spaceport operated by another space agency.[138] Russia has also indicated its interest in continuing its partnership with the United States after the ISS retires.[139]

While largely successful, the Russian space industry has also been plagued with serious corruption scandals. In 2018, Russia's principal federal investigation authority discovered that fraud cases within the country's space and defense industry reached $1 billion.[140] Roscosmos, the Russian space agency, has been particularly wrought with corruption. Last year, a high-level agency official—who was likely linked to an internal embezzlement scheme—fled the country to Europe while he was under investigation.[141] Also in 2019, 58 people received jail sentences after $172 million was stolen from the Vostochny spaceport in the Russian Far East.[142] Only a fraction of the monies lost had been recovered as of November 2019. When asked about the culture of corruption at Roscosmos, the director of the Russian Investigative Committee said "there is no end in sight."[143]

In light of these issues, Roscosmos has announced extravagant spaceflight plans for the upcoming decade. In a presentation to students at Moscow University in May 2019, the agency's director announced the country's plans to invest in a new crewed space vehicle with flights to the ISS by 2023, develop a new heavy-lift launch vehicle, and even land cosmonauts on the Moon by 2030.[144] The scale of these new missions would almost certainly require the country to increase its budget for space activities, likely putting the space agency at odds with other federal spending priorities.[145]

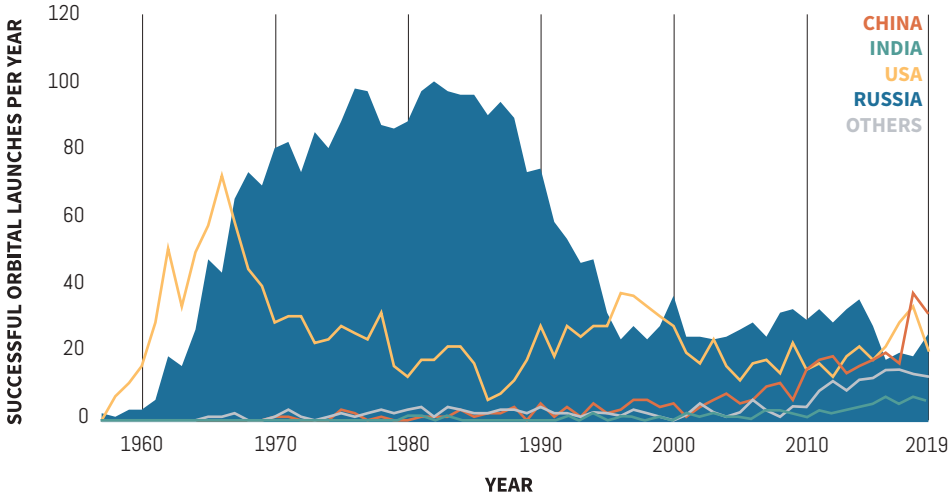


Figure 7: Russian Orbital Space Launches (1957-2019).

SPACETRACK.ORG / CSIS AEROSPACE SECURITY[148]

SPACE ORGANIZATION AND DOCTRINE

Most state-sponsored space activities in Russia are linked to one of two government organizations: Roscosmos, the country's civilian space body, and the Russian Aerospace Forces, the branch of the Russian armed services tasked with military operations in the space domain. Roscosmos, known as the Russian Federal Space Agency until 2015, inherited significant space infrastructure from its predecessor, the Soviet space program.[146] Tasked with the pursuit of international cooperation with space partners around the world, Roscosmos is one of five principal partners that support the ISS, along with civilian space agencies in the United States, Japan, Canada, and Europe.[147]

When the Russian Ministry of Defense was created in 1992, Russia established the world's first space force.[149] Now known as the Russian Space Forces subbranch—a part of the broader Russian Aerospace Forces—the Russian Space Force is responsible for launching military satellites, maintaining space-based assets, monitoring space objects, and identifying potential attacks against the Russian homeland from space.[150]

Russia considers the "intention to place weapons in outer space" a main external military danger and describes establishing "an international treaty on [the] prevention of placement of any types of weapons in outer space" as a principal task for the Russian state in its military doctrine.[151] Although Russia and China co-submitted the "Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force Against Outer Space Objects" to the Conference on Disarmament in 2008, the United States dismissed the proposal as a "diplomatic ploy," and refused to support it.[152] In 2014, Russia and China reintroduced the treaty, prompting a similarly chilly reaction from the United States. In response to the Indian ASAT

test in March 2019, the Russian Ministry of Defense acknowledged India's otherwise strong dedication to preventing an arms race in space while simultaneously blaming the United States for creating an environment in which developing space actors are compelled to test anti-satellite weapons on orbit—a clear jab at U.S. opposition to Russia and China's failed treaties.[153]

Although Russia's military doctrine has not been publicly updated since December 2014, some analysts expect a new version may be released later this year.[154] Since the last military doctrine was released, Dmitry Rogozin—the Roscosmos director general and former deputy prime minister for defense—has stated that Russia does not use satellites to damage other space objects.[155] More recently, Russian military leaders have suggested that the Trump administration's support of the U.S. Space Force warrants new "reciprocal and asymmetrical measures" from Russia in the space domain.[156] In a December 2019 address, Russian President Vladimir Putin stated that the creation of a U.S. Space Force requires Russia to further invest in its own military space industry.[157]

COUNTERSPACE WEAPONS

Kinetic Physical

Evidence suggests that Russia has invested in a sweeping range of kinetic physical counterspace capabilities over the past decade, including ground- and air-launched direct-ascent ASAT missiles capable of targeting satellites in LEO and co-orbital ASAT weapons that could operate in any orbital regime. Russia's kinetic physical counterspace activities often closely resemble previously operational Soviet-era ASAT programs, suggesting that the country has benefited from decades of ASAT weapons research conducted by the Soviet Ministry of Defense.

On October 20, 1968, the Soviet Union became the second country in the world to successfully demonstrate a counterspace weapon when it destroyed a domestic satellite in LEO using a co-orbital ASAT. Called *Istrebitel Sputnikov (IS)*, meaning "satellite destroyer" in Russian, the first Soviet co-orbital ASAT was tested 20 times between 1963 to 1982, destroying several targets launched as part of the program.[158] A follow-on version of the *IS* system, known as IS-MU, was operational from 1991 to 1993.[159]

Prior to the fall of the Soviet Union, the country began developing a much more capable co-orbital ASAT known as the *Naryad*. Reportedly designed to reach altitudes as high as 40,000 km and contain multiple warheads in a single launch, the *Naryad* would likely have posed a serious threat to satellites in GEO.[160] The system saw limited testing—with just one launch in 1994—and no confirmed intercepts.[161]

Unlike the Soviet Union, Russia's kinetic physical counterspace arsenal includes ground-launched direct-ascent ASAT missiles. In December 2018, Russia conducted its seventh test of the PL-19/*Nudol* direct-ascent ASAT system.[162] The PL-19/*Nudol* completed its first successful flight test in November 2015, after two unsuccessful attempts.[163] Unclassified U.S. reports suggest that both this launch, and a previous test in March 2018, used a mobile transporter erector-launcher (TEL) within the Plesetsk Cosmodrome complex instead of a static launch pad.[164] Although at least six of the seven launches are verified to have originated from Plesetsk, a mobile launch system would theoretically allow the ASAT to be launched outside of the Cosmodrome facility, ensuring greater flexibility to target LEO satellites in inclinations above 40 degrees as they transit over Russian territory.[165]

Although not specifically designed as direct-ascent ASAT weapons, Russian mobile-launched S-400 surface-to-air missiles—capable of reaching a maximum altitude of 200 km—could potentially reach a satellite in LEO. The follow-on surface-to-air missile system, the S-500, is expected to reach altitudes up to 300 km if launched directly upward.[166] Oleg Ostapenko, Russia's former deputy minister of defense, once stated that the S-500 will be able to intercept "low-orbital

satellites and space weapons."[167] First tested in 2018, the new missile's production timeline has since slipped, and "there has been no indication of when an actual S-500 will be made available."[168] Like the PL-19/*Nudol* system, using the S-400 or eventually the S-500 as a direct-ascent ASAT would require a high-precision targeting capability that has yet to be demonstrated via a destructive test.[169]

A modified Russian MiG-31 fighter jet was photographed in September 2018 carrying an unidentified missile that some reports suggest could be a "mock-up" of an air-launched ASAT weapon.[170] Although this development follows a 2013 statement from the Russian Duma expressing the Russian government's intent to build an air-to-space system designed to "intercept absolutely everything that flies from space," the system depicted in the September 2018 photo would almost certainly be limited to targeting objects in LEO, due to its size.[171] In 2017, a Russian Aerospace Forces squadron commander confirmed that an ASAT missile had been designed for use with the MiG-31BM aircraft—the same variant spotted with the mysterious missile.[172] Citing several sources familiar with a U.S. report on the new weapons system, CNBC reported that the missile may become operational as soon as 2022.[173]

Russia has not publicly announced the development of a new co-orbital ASAT program since the fall of the Soviet Union. In the past few years, however, the Russian Aerospace Forces has launched a series of small "inspector" satellites in LEO that have demonstrated some of the technologies required to operate such a system. In 2017 and 2018, three small Russian satellites—Cosmos 2519, 2521, and 2523—engaged in RPO in LEO, prompting a statement of concern from the U.S. State Department.[174] Although a June 2017 Russian Soyuz launch appeared to place just one satellite in LEO—Cosmos 2519—a second satellite was detected two months later, likely deployed from the first as a subsatellite.[175] The Russian Ministry of Defense made a statement saying that the second satellite was designed to "inspect the state of a Russian satellite."[176] In October 2017, a third satellite was deployed from either Cosmos 2519 or its subsatellite, resulting in three independent satellites in orbit. Over the course of several months, the satellites engaged in a series of maneuvers and RPO exercises, including slow flybys, close approaches, and rendezvous. In February 2020, Chief of Space Operations of the U.S. Space Force General John Raymond appeared to refer to one of these three satellites when he said that Russian inspector satellites have "exhibited characteristics of a weapon."[177]

Analysis published in *Jane's Intelligence Review* used Russian procurement documentation and contractor reports to connect Cosmos 2519, 2521, and 2523 with the program name *Nivelir*.[178] Contracts signed in 2016 between the *Nivelir* program and a Russian company known for developing radiation-absorbing materials suggest that future *Nivelir* satellites—such as Cosmos 2535, 2536, 2537, or 2538, all launched in July 2019—may be coated with a protective film to avoid being tracked by optical or infrared sensors from the ground or in space.[179]

MiG-31BM "Foxhound" Aircraft on September 14, 2018. Photographed at the Zhukovsky airfield outside of Moscow, the aircraft is carrying what has since been identified as a potential anti-satellite weapon.
SHIPSASH / JETPHOTOS.COM

Spying on a Spy Satellite

ON NOVEMBER 25, 2019, Russia launched a small satellite, Cosmos 2543, into what the Russian Ministry of Defense described as a "target orbit from which the state of domestic satellites can be monitored."[180] Two weeks later, the ministry announced that a subsatellite, Cosmos 2542, had been deployed from Cosmos 2543.[181]

Three days after its deployment, Cosmos 2542 performed an orbital maneuver to synchronize its orbit with USA 245, what is believed to be a U.S. National Reconnaissance Office (NRO) satellite. Amateur satellite observers who record and share satellite observations online noticed that USA 245 performed its own maneuver soon thereafter, possibly to steer clear of Cosmos 2542.[182] In January 2020, Cosmos 2542 maneuvered toward the American spy satellite again, this time coming as close as 50 km.[183] A day later, USA 245 made another maneuver, further distancing itself from the Russian inspector satellite.[184]

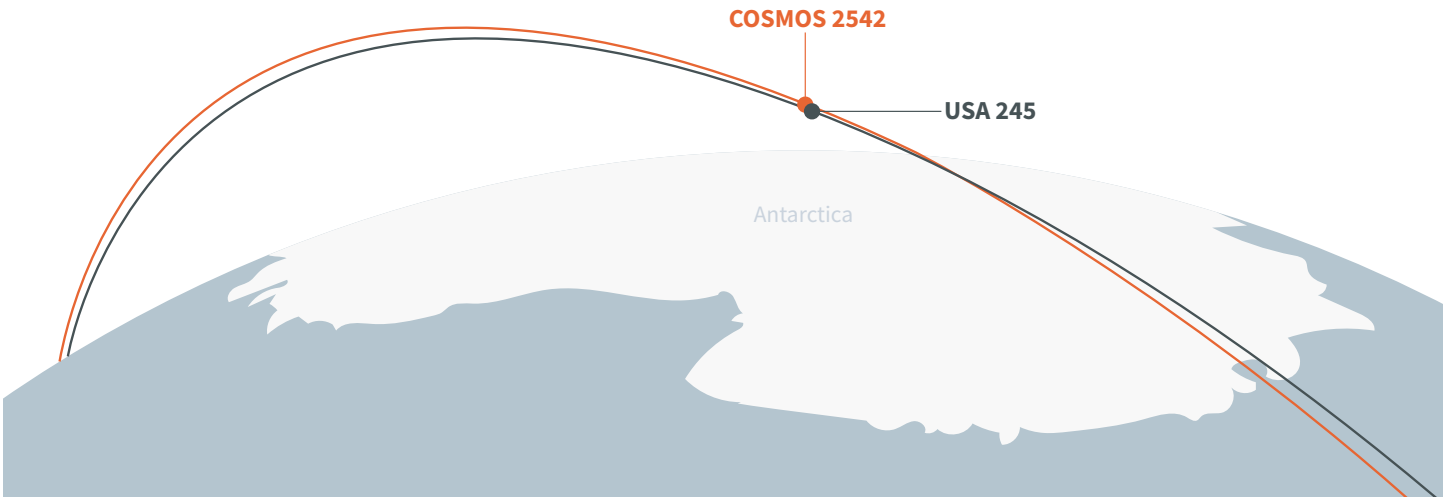
In an interview with *SpaceNews*, General John Raymond, the Commander of U.S. Space Command and Chief of Space Operations of the U.S. Space Force, confirmed the close approach, adding that he believed it was intentional.[185]

Figure 8: Orbital Trajectories for Cosmos 2542 and USA 245 on January 23, 2020. Since orbital parameters for classified satellites do not appear in the U.S. Space Command's public catalog of space objects, analysts use observations from amateur astronomers to calculate USA 245's orbital trajectory.

NICO JANSSEN / SATOBS.ORG

Russia's newest co-orbital system may be designed to target satellites in GEO.[186] Designated *Burevestnik*, this program will likely employ low-thrust but highly-efficient electric propulsion to maneuver lightweight satellites—possibly similar to those from the *Nivelir* program—around the GEO belt.[187] A report published in 2019 indicated that a new ground control center was being built for *Nivelir* and *Burevestnik* at the same site the Soviets used to control the *Istrebitel Sputnikov* missions in the 1960s.[188]

Although there is no evidence yet of lightweight Russian satellites maneuvering in the GEO belt, a larger satellite has been observed engaging in suspicious RPO activity in the regime. The satellite—known as *Olymp-K* or *Luch*—has attracted attention for shifting its position within the geosynchronous belt on a relatively frequent basis, occupying at least 19 different positions since its launch in September 2014.[189] *Luch* first attracted attention when it repositioned itself between two satellites operated by Intelsat, a U.S. satellite communications company.[190] Approaching satellites in GEO in this manner could allow for close inspection or potentially interception of their communication links.[191] In September 2015, *Luch* approached a third Intelsat satellite.[192] The international response escalated in September 2018, when French Minister of the Armed Forces Florence Parly accused Russia of committing "an act of espionage" after it approached a French-Italian military satellite "a bit too closely" in October 2017.



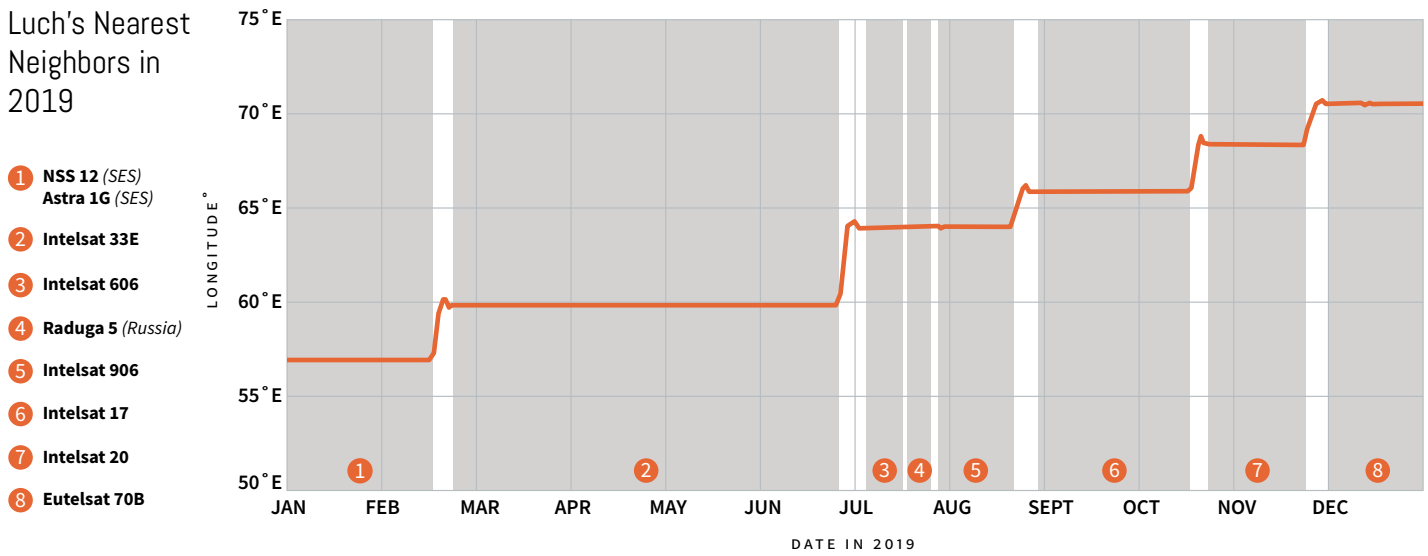


Figure 9: Luch Continues to Explore the GEO Belt. The Russian satellite has stopped at 19 different positions in the geostationary belt since its launch in 2014, including those depicted here in 2019. Learn more about Luch's behavior, including a list of the satellite's nearest neighbors at aerospace.csis.org/luch.

SPACE-TRACK.ORG / CSIS AEROSPACE SECURITY

Analysis of *Luch*'s on-orbit behavior since its launch in 2014 suggests that the satellite has approached 11 unique Intelsat satellites, four Eutelsat satellites, two SES satellites, and at least nine other satellites operated by Russia, Turkey, Pakistan, the United Kingdom, and the European Space Agency.[193] Although *Luch* appears to be maneuvering around the GEO belt in a systematic, deliberate manner, no public reports suggest it has damaged any of the neighboring satellites along the way.

Non-Kinetic Physical

Evidence suggests that Russia has both maintained its non-kinetic physical counterspace capabilities from the Soviet era—including detonating nuclear weapons at high altitudes, using nano-sized obscurants on orbit, and placing laser weapons on aircraft—and built upon them over the past 10 years.

In 1962, the Soviet Union detonated three nuclear warheads about 400 kilometers above the Earth's surface—near the altitude of the U.S. Starfish Prime test that same year—in a series of tests known as Operation K.[195] As suspected by the Soviet engineers who planned the tests, Operation K demonstrated the devastating effects of an EMP weapon in LEO. Though nuclear warheads were tested as part of the early *Istrebitel Sputnikov* tests, the program's successful intercepts used conventional warheads instead, which lowered the risk of inadvertently damaging Soviet satellites on orbit during testing.[196] Thirty years later, Vladimir Lukin, a senior Russian legislator, reminded the international community of Russia's retained EMP capabilities when he threatened a delegation of U.S. congressmen during an official visit in May 1999, saying:

> *Hypothetically, if Russia really wanted to hurt the United States . . . [it] could fire a submarine launched ballistic missile and detonate a single nuclear warhead at high-altitude over the United States. The resulting electromagnetic pulse would massively disrupt U.S. communications and computer systems, shutting down everything. No internet. Nothing.*[197]

"We have achieved significant progress in laser weapons."

VLADIMIR PUTIN, RUSSIAN PRESIDENT [194]

Academic articles, government contracts, and patent documentation suggest that Russia is sponsoring scientific research into on-orbit aerosol obscurants—nanoparticles that can block radiofrequency and optical signals to and from a satellite—which could be used to hide Russian satellites from space situational awareness sensors on the ground or as part of an offensive co-orbital attack.[198] According to analysis published by the website Space Review, Russia's Scientific Research Institute of Applied Chemistry (NIIPKh), known for its previous work in aerosol particle development, was awarded a contract from the previously-discussed *Burevestnik* program in 2015. Although there is no evidence that particle obscurants have been tested on orbit, an article written by NIIPKh affiliates in 2016 suggested that the technology could be installed on satellites, where it could be used to defend assets from kinetic physical attacks but also for "disabling" satellites from a close distance.[199] If deployed from a nearby satellite, particle obscurants could be used to temporarily degrade a target satellite by obstructing optical sensors or interfering with radio communications to and from its ground stations.

Leaked photos, statements from Russian defense contractors, and Russian news reports suggest that a Soviet-era laser weapon from 1965 has been revived to target satellites in LEO.[200] In 2011, photos of a modified *Ilyushin Il-76MD* cargo plane, known as the *Beriev A-60*, featuring what appears to be an upward-facing laser on the fuselage and a targeting system built into its nose cone, were uploaded to an online forum for Russian plane enthusiasts. The system, known as *Sokol Eshelon,* was likely tested two years earlier to illuminate a Japanese satellite on orbit at an altitude of 1,500 km.[201] In 2017, the general director of Almaz-Antey, a weapons manufacturer with ties to the program, told a Russian news outlet that his company had been ordered to develop a system capable of "direct functional destruction of those elements deployed in orbit."[202] A year later, however, Interfax reported that Almaz-Antey had finished work on a new air-based laser ASAT system that would most likely rely on a "fundamentally new aircraft [that is] not based on the Il-76MD."[203] Regardless of the aircraft on which the laser weapon is mounted, such a weapon could be capable of damaging its targets' optical sensors and solar arrays from anywhere in Russia's vast airspace.

In a presidential address in March 2018, Russian President Vladimir Putin announced the development of a new directed-energy weapon.[204] Russian news outlets later reported that the ground-based laser weapon, known as *Peresvet*, was first delivered to Russian troops in July 2017 and had been placed on "experimental combat duty" in December 2018.[205] A video released by the Russian Ministry of Defense shows the weapon mounted on a trailer, suggesting some degree of mobility.[206] Russian officials told reporters that the system is distributed over two platforms, with the second responsible for the laser's power source. Yury Borisov—former Russian deputy minister of defense, now the country's deputy prime minister—commented that *Peresvet* would be made more compact over the next two to three years.[207] President Putin recently announced that the weapon would be placed "on standby alert" in December 2019.[208] Although the most critical details about *Peresvet* remain unknown.[209]

Electronic

The Russian government has been accused of widespread GPS jamming and spoofing since 2014, affecting civilian and military vessels near Russian territory, commercial and civilian aircraft in the Arctic Circle, and handheld consumer devices in downtown Moscow and St. Petersburg.[211] Despite overwhelming evidence that Russia has employed the use of mobile, ground-based electronic counterspace weapons on a regular basis both within its borders and abroad, the Russian state has repeatedly denied any wrongdoing.[212]

Since the beginning of the 2014 Crimean conflict, Russia has used a variety of jamming and radio-monitoring platforms—

"GNSS [Global Navigation Satellite System] spoofing activities in the Russian Federation, its occupied territories, and its overseas military facilities are larger in scope, more geographically diverse, and started earlier than any public reporting has suggested to date."

CENTER FOR ADVANCED DEFENSE STUDIES[210]

The Trailer-Mounted *Peresvet* Laser Weapon System. Some observers suspect that the laser's power levels will allow it to target satellites in LEO.

RUSSIAN DEFENSE MINISTRY

including the truck-mounted R-330Zh jammer and the R-381T2 radio monitoring system—to deny Ukrainian forces access to consistent GPS and satellite communication services.[213]

Similarly, Russia reportedly deployed a *Krasukha-4* truck-mounted jamming system in Syria, another conflict region, and supplied the Syrian army with R-330P radio jammers.[214] Using sensor data from the International Space Station, analysts at the Center for Advanced Defense Studies (C4ADS) and the University of Texas at Austin identified "potential military-grade EW systems" likely designed for "airspace denial purposes" at Khmeimim airbase, a Russian-operated air base in western Syria.[215]

Russia's use of electronic counterspace weapons is not restricted to conflict zones. Starting in late 2017, civilian and commercial aircraft operators in the northernmost region of Norway—Finnmark County, which borders Russia's Murmansk Oblast—began reporting recurring GPS signal outages during flight.[220] Analysis of notice to airmen (NOTAM) alerts distributed from September 2017 to January 2019 shows a correlation between GPS signal outages and military exercises in the region, including a Russian-Belarusian joint exercise in Russia in 2017, a NATO exercise in Norway, Sweden, and Finland in 2018, and a nearby British exercise in 2019. After Norway announced that Russia was responsible for the regional jamming incidents, the Norwegian Communications Authority made plans to establish a satellite signal measurement station to better understand the GPS jamming environment in the region.[221]

In 2017, over 20 ships operating in the Black Sea reported gross GPS position errors as they sailed near the Russian coast.[222] The incidents were first reported by the U.S. Maritime Administration. A C4ADS report from March 2019 identified hundreds more "denial-of-service" occurrences in the region from both before and after the original report where onboard GPS devices were calculating false coordinates for the vessels.[223] In many cases, GPS devices calculated ships' positions as being at a nearby Russian airport, and not in the Black Sea. The report—a collaborative study between C4ADS, the University of Texas at Austin, and Palantir Foundry—also suggested a specific location for at least one of the spoofing devices responsible: "a multi-million dollar 'palace,' formerly owned by family members of senior Federal Protective Service officers and previously reported to be built for President Putin."[224] The FSO is the Russian counterpart of the Secret Service in the United States, a federal agency responsible for senior government leaders' personal security.

The C4ADS report suggests that the FSO's relationship with Russia's use of electronic counterspace weapons does not stop at the seaside palace. The report identified 12 occurrences in which evidence of one-off PNT spoofing events corresponded with the movements of Russian President Vladimir Putin, his senior advisers, or FSO officers, suggesting that "some devices used to conduct this activity are mobile and can be temporarily deployed at a location to create local areas of effect."[225]

A $4,000 Taxi to the Kremlin

IN JUNE 2016, visitors to downtown Moscow began noticing a problem with their mobile devices' mapping services.[216] When driving or walking near the Kremlin, at the center of the city, users reported being directed to follow implausibly inefficient routes. In some cases, mapping software suggested a detour of just a few blocks. In others, mobile device users were directed as far away as the Vnukovo Airport, almost 50 kilometers southwest of the Kremlin.[217] Visitors were particularly affected when using ride-sharing services, complaining on Twitter about $3,000 to $4,000 fare estimates due to the mapping errors.[218]

These map users were likely receiving false positioning signals, leading them to specific, incorrect locations away from the Kremlin. Residents of St. Petersburg began reporting similar issues during a visit from President Vladimir Putin in December 2016.[219]

Figure 10: Russian President Vladimir Putin Visiting the Newly Constructed Crimean Bridge Connecting Crimea to Mainland Russia on May 15, 2018. Denial-of-service reports from vessels near the bridge at the time of the visit suggest that a spoofing device may have been contained in one of the orange construction trucks that made up the president's motorcade.

ALEXANDER NEMENOV / AFP / GETTY IMAGES

In two of those cases, the Russian president was visiting the newly-constructed Crimean Bridge, which physically connects Crimea with the Russian mainland. On May 15, 2018, the second of those two visits, President Putin celebrated the project's completion by driving across the bridge in a motorcade of construction vehicles. Based on the locations of the ships experiencing GPS spoofing at the time—which typically must be within the line of sight of the spoofing device feeding them false coordinates—it is possible that the spoofing device was contained in one of the vehicles in Putin's motorcade.

Several months after Putin's visit, the Crimean Bridge was the site of a military conflict in which Russia was accused of using electronic weapons. In November 2018, the Russian Coast Guard opened fire on three Ukrainian Navy ships as they attempted to pass underneath the Crimean Bridge from the Black Sea into the Sea of Azov, in what became known as the Kerch Strait incident. A month after the incident, which injured six sailors according to Ukraine, Ukrainian Navy Commander Ihor Voronchenko accused Russia of spoofing GPS signals and jamming access to the Iridium satellite communications network.[226]

In 2016, Russia announced plans to install GPS jammers on the country's 250,000 cell phone towers.[227] The system, called Pole-21, is aimed at providing more widespread GPS jamming to protect Russian assets against cruise missiles, drones, and precision-guided munitions. In November 2019, the Russian military confirmed that the first units have been delivered.[228]

Russian electronic counterspace activities may not be limited to ground-based systems. Late last year, Russian news reports suggested that the Russian Aerospace Forces may upgrade its *Porubshchik* electronic warfare aircraft, which could be used to jam satellite signals across wider regions than a truck- or tower-mounted jamming device.[229] Although there is no evidence in the public domain that Russia employs space-based electronic counterspace weapons, analysis of Russian procure-

ment documentation from 2014 points to a new program called *Ekipazh* that may feature a nuclear-powered jamming device on orbit.[230] Early reports from the program's manufacturers suggest that test flights could begin as early as 2021.

Cyber

Foreign governments regularly accuse Russia of widespread international cyberwarfare.[231] In the space domain, a group of hackers with links to the Russian Federal Security Service called *Turla* has been hijacking the internet services of older commercial satellites since 2007.[232] More recently, from 2017 to 2019, *Turla* infiltrated government agencies and private companies in more than 20 countries according to reports from the British National Cyber Security Centre and U.S. National Security Agency.[233] During the attacks, the group attempted to disguise themselves as an Iranian hacking organization by first gaining access to computer infrastructure previously associated with Iranian cyberattack operations. In April 2015, a French satellite TV network was pulled off the air in an attack linked to another Russian hacker group known as APT 28.[234] Later that year, APT 28 gained access to a British television station's computer network, but did not tamper with any of its broadcasted programming.[235]

Russian cyberattacks on state governments and international organizations extend well outside of the space domain, earning criticisms from Estonia, Ukraine, the United States, the United Kingdom, France, Germany, Kyrgyzstan, and the Netherlands.[236] In August 2019, NATO Secretary General Jens Stoltenberg specifically addressed Russia's nefarious activities in the cyber domain in an editorial about NATO's renewed cybersecurity efforts. No other state perpetrators were mentioned.[237] Russia's Ministry of Foreign Affairs has developed a consistent pattern of denying accusations of wrongdoing in the cyber domain, calling the negative attention "stage-managed propaganda campaign[s]" and "Western spy mania."[238]

SUMMARY

While the Soviet Union developed weapons in just two of the four counterspace categories—kinetic and non-kinetic physical weapons—Russia has invested in all four over the past 10 years. Evidence suggests that Russia is developing an air-launched direct-ascent ASAT missile, has already tested a ground-based direct-ascent ASAT, and is reinvigorating an array of co-orbital counterspace technologies more than 50 years after the Soviet Union became the first and only country to successfully destroy a target satellite using a co-orbital ASAT weapon. Russia has built off of the Soviet Union's arsenal of non-kinetic counterspace weapons by reviving a Soviet-era air-based laser weapon and unveiling a new ground-based trailer-mounted laser weapon. In just the past few years alone, Russia has become one of the world's greatest perpetrators of electronic counterspace warfare, jamming and spoofing PNT and communications satellite signals in conflict zones, nearby territories, and within its own borders. Although difficult to verify, Russia is also almost certainly capable of targeting satellites and associated ground stations through vulnerable computer networks. With new weapons added to the Russian counterspace arsenal each year since 2018, it is clear that the country has renewed its focus on developing and maintaining its ability to disrupt, degrade, or destroy adversaries' assets on orbit.[239]

Number of Successful Orbital Launches in 2019[240]

0

IRAN

"The United States will not allow Iran to use its space launch program as cover to advance its ballistic missile programs,"

MIKE POMPEO, U.S. SECRETARY OF STATE[241]

OFTEN CITED AS A THINLY VEILED COVER for its ballistic missile program, Iran's space capabilities are relatively minimal.[242] Iran's space and ballistic missile systems are likely based on Russian and North Korean programs. This analysis is supported by the weak aerospace industrial base in the country, suggesting that Iran is unlikely to have the technical and industrial capability to develop complex launch technology from scratch.[243] In 2009, Iran successfully launched its first domestically-manufactured satellite on a *Safir-1* rocket, making it the ninth country at the time to have launched an indigenous satellite.[244] The Iranian Space Agency (ISA) continues to claim to have sent various living creatures into space in the last decade, including a monkey two times in 2013.[245] The agency had previously aimed to put a human in space by 2025, but human spaceflight aspirations were put on hold in 2017 due to budget constraints, likely linked to U.S.-imposed sanctions. However, the ISA has continued to focus on improving its SLVs.[246]

Iran's main launch facility, the Imam Khomeini Spaceport, is located in a larger domestic space facility, the Imam Khomeini Space Center, in the Semnan Province east of Tehran. The site is also used as one of eight missile test and launch sites in the country.[247] Iran had four successful launches from 2009 to 2015 that put various operational satellites into orbit, none of which stayed in orbit longer than a few months.[248] In 2014, Iran reportedly signed an agreement with Russia for its assistance in the development and launch of Iranian satellites and possibly the training of future Iranian astronauts.[249]

"Iran recognizes the strategic value of space and counterspace capabilities."

U.S. DEFENSE INTELLIGENCE AGENCY

The U.S. Intelligence Community has assessed that "Iran recognizes the strategic value of space and counterspace capabilities" and that continued work to develop space launch vehicles will shorten the timeline to create a successful ICBM.[250] Iran is an unusual case as countries have historically constructed space launch capabilities from military ballistic missile programs, not the other way around.[251] In addition to SLVs, Iran has also developed space capabilities with military applications such as a space monitoring center announced in June 2013 that uses radar, electro-optical, and radio tracking.[252] Iran continues to focus on space situational awareness monitoring, announcing in 2018 that experts built radars which can monitor satellites in LEO.[253]

Iran currently has two known launch vehicles, the *Safir-1* and *Safir-2*, the latter of which is commonly known as the *Simorgh*.[254] While the *Safir-1* has had successful orbital launches, the *Simorgh* has yet to complete a fully successful mission.[255] In July 2017, Iran announced a successful test launch of the *Simorgh*, although the success of the test has not been confirmed outside of state media.[256] For the Iraninan space program, 2019 proved to be a difficult year, with three failed orbital launches in January, February, and August, which used alternately the *Safir-1* and *Simorgh* launch vehicles.[257]

Failed Launch Attempt

ON AUGUST 25, 2019, the head of the Iran Space Agency was quoted in state media saying that the agency planned to launch three satellites into orbit by March of 2020. The goal of these three satellites would be to help aid civilians through improving navigational, agricultural, and environmental monitoring services.[258] Four days later, on August 29, satellite imagery from the Earth-imaging company Maxar Technologies showed a launch pad at the Imam Khomeini Space Center that appeared to be the aftermath of a failed launch attempt. Satellite imagery analysts were able to note that the pad had been recently painted, likely for the launch itself and to cover up previous damage from failed launches, with smoke billowing from the ground, indicative of a failed launch. An anonymous Iranian official admitted to Reuters that the incident was caused by technical issues but would not go into further detail.[259]

President Trump tweeted a high resolution image of the scarred launch pad, underscoring that the United States was not involved.[260] Although Iran has continued to claim its space program is peaceful, that has not always been the belief of the U.S. government, whose officials often remark that the space program may be a front for developing Iranian ballistic missiles.[261] Days after this third failed launch attempt of the calendar year, the Trump administration added the Iran Space Agency, the Iranian Astronautics Research Institute, and the Iran Space Research Center to the U.S. sanctions list.[262]

New satellite images surfaced in January 2020 which showed the launch pad being repaired, possibly in preparation for another launch attempt with a *Simorgh* launch vehicle.[263] This timing coincided with statements from the Iranian Minister of Information and Communications Technology, who announced that the program had six satellites ready to launch. He announced that two are communications satellites, named *Zafar-1* and *Zafar-2,* were reportedly ready for a launch in early February.[264] On February 9, 2020, the *Simorgh* rocket launched with a satellite on board, but the satellite did not reach high enough velocity to stay in orbit. A spokesman for the Iranian defense ministry's space program claimed that the Simorgh functioned properly, calling it a "remarkable" feat for the space program. The minister of Information and Communications Technology continued by saying the program is "UNSTOPPABLE! We have more Upcoming Great Iranian Satellites!"[265]

Figure 11: Satellite Image of Iranian Launch Attempt on August 25, 2019.

CSIS / MAXAR TECHNOLOGIES

SPACE ORGANIZATION AND DOCTRINE

Iran was one of the founding members of the UN Committee on the Peaceful Uses of Outer Space in 1958; however, the country is one of many that has signed but not ratified the Outer Space Treaty.[266] The Iranian Space Agency was established in 2004 ostensibly to coordinate peaceful applications of space activities and technology development for the country.[267] The agency is under the oversight of the Ministry of Information and Communications Technology, but takes direction from the Supreme Space Council, which is chaired by the president of Iran. The head of the space agency serves as the secretary of the Supreme Space Council, which is overseen by the president and focuses on making policy for peaceful space technologies, approving state and private space programs, and promoting domestic, private, and international cooperation in space issues.[268]

The Iranian Space Agency also runs the Iranian Space Research Center and reportedly has planned to establish a "space park," a space-themed center that focuses on education, culture, recreation, and amusement. The park would be run in partnership with the Sharif University of Technology (SUT), a well-known research university that supports the government in ballistic missile-related projects.[269] Little is publicly known about Iran's doctrine for space and counterspace operations, but evidence suggests that Iran believes the capability "to deny the United States the ability to use space in a regional conflict" is critical to its security.[270] Although the country often uses aggressive rhetoric when discussing ballistic missile activities, Iran consistently claims that its space program is peaceful.[271]

Budgets for the Iranian Space Agency have risen in the last decade. In 2010, the space agency had a reported budget of $1.5 million, which the minister of Communications and Information Technology enthusiastically reported saying "being in space is one of the key factors in the power of governments."[272] In 2017, the budget for the space agency was reported to be $4.6 million.[273] The space agency's budget is separate from Iran's military spending, which has increased by over 50 percent in the last five years, swelling to 7.5 percent of its total national budget for 2018–2019.[274] Though Iranian leadership takes steps to obscure the specifics of its military budget, priorities include improving domestic missile production capabilities. Because of limited domestic capability to produce reliable components, Iran continues to rely on imported components and materials for their missiles. Iran is not a major space power in terms of proven space capabilities, but it continues to invest in and develop significant counterspace capabilities.

COUNTERSPACE WEAPONS

Kinetic Physical

While currently available open-source information does not indicate that Iran is attempting to develop either direct-ascent or co-orbital ASAT weapons, Iran has some of the ballistic missile technology on which a future direct-ascent kinetic ASAT capability could be based. In addition to a diverse set of ballistic missile programs with varied ranges, Iran has substantial conventional forces, with an estimated 523,000 active personnel.[275] Iran's ballistic missile capabilities include the *Shahab-3*, which is believed to be derived from the North Korean *No Dong-1* missile.[276] The *Simorgh* SLV is similarly based on the North Korean *Taepo Dong-2,* including modeling *No Dong-1* engines.[277] Iran appears to have been able to reproduce these missiles in quantity, which led U.S. Secretary of State Mike Pompeo to publicly assert that "Iran has the largest ballistic missile force in the Middle East."[278]

Iran has demonstrated the rudimentary ability to launch and operate primitive satellites for short periods of time, and its space monitoring center gives it the ability to track objects and have better space situational awareness.[279] Having a reliable understanding of where objects are in space is required for targeting many capabilities. However, there are many other technological hurdles to tackle before Iran could field a direct-ascent kinetic ASAT weapon, such as precise onboard sensors that could guide a warhead into a target satellite.

Realistically, Iran could construct a crude direct-ascent ASAT capability by modifying an existing ballistic missile and launching it within the vicinity of a target satellite with an unguided warhead. It would not likely be able to hit a specific satellite but could create a debris hazard in the space environment that threatens the safety of numerous other satellites in similar orbits.

During a military parade in late 2019, Iran unveiled a new indigenous ballistic missile kit design, the Labbayk-1, which aims to modify unguided short-range *Zelzal* and *Fateh-110* ballistic missiles into guided weapons.[280] This new capability could lead to an increase in accuracy, as demonstrated in recent Iranian surface-to-air and air-to-air missile attacks in the Middle East.[281] This increased capability may pose a threat to space systems by being able to more reliably attack satellite ground stations throughout the Middle East and Europe.[282]

Non-Kinetic Physical

There are few reports of Iranian non-kinetic physical weapons, but the country may have acquired and used a laser dazzling or blinding counterspace system on a U.S. satellite. In 2011, an unnamed European intelligence source was quoted stating that Iran managed to "blind" a U.S. satellite by "aiming a laser burst quite accurately."[283] The technology necessary to do this, particularly the adaptive optics needed to steer and focus a laser as it passes through the Earth's atmosphere, is quite sophisticated, indicating that Iran may have obtained this technology from Russia or China. Its capabilities in this area remain highly uncertain based on the limited publicly available information.

If Iran were to continue pursuing a breakout nuclear capability, it is conceivable that it could launch a nuclear weapon into orbit as a nuclear ASAT capability. In the 1990s, Iran entered into agreements with both China and Russia to help jumpstart its nuclear program. China agreed to include the training of Iranian personnel and contribute various reactor technologies.[284] Iran has also entered into a bilateral nuclear cooperation agreement with Russia to provide nuclear experts, information, and aid in the completion of Iran's first nuclear power plant. [285]

Recently, the program has leaned most heavily on North Korean cooperation. In 2012, Iran and North Korea signed the Civilian Scientific and Technological Cooperation Agreement, which established joint facilities and a "transfer [of] technology" in multiple fields.[286] Former Special Coordinator for the State Department's North Korea Group, David Asher, added "the last time North Korea signed an agreement like this it led to the largest act of nuclear proliferation in modern history."

Development of Iranian nuclear capability was temporarily slowed in 2015 by the Joint Comprehensive Plan of Action (JCPOA).[287] The United States pulled out of the JCPOA in 2018, and after a series of international events which increased tensions between the two nations, Iran also stated it would no longer adhere to the deal.[288] The remaining countries involved in the JCPOA, including Russia and China, hope to reimplement the agreement.[289] Despite pulling out of the JCPOA, President Trump reiterated as recently as January 2020 that Iran would "never be allowed to have a nuclear weapon."[290] However, the aim of Iran's nuclear program has historically been to develop a nuclear-armed ICBM to deter the United States, not a nuclear counterspace ASAT weapon.

Electronic

Jamming and spoofing are regular tools in Iran's weapons arsenal. In 2003, Voice of America (VOA) broadcasts into Iran began to experience interference with its transmissions over the Telestar-12 satellite. The uplink jamming of this commercial satellite originated from the area around Havana, Cuba. The U.S. State Department notified Cuba of the issue, and subsequently determined that the source of the jamming was from a compound belonging to the Iranian Embassy. Cuban authorities promptly shut down the facility and issued a note of protest to the Iranian government.[291] Similar attacks emanated from Bulgaria and Libya from 2005 to 2006. Though Iran's role went unconfirmed, "international pressure eventually brought this to a halt and satellite jamming against Persian-language programming now emanates exclusively from Iranian territory."[292]

> "We have been equipped with electronic warfare systems in order not to remain just a defending force, and rather become able to jam the enemy's communication systems,"
>
> BRIGADE GENERAL AHMADREZA POURDASTAN[293]

Iran has also jammed several international and regional television broadcasts in the Middle East. In 2010, Iran jammed BBC and VOA satellite signals transmitting into Iran. At first, the jamming tar-

IRAN HAS DEMONSTRATED ITS CYBER CAPABILITIES BY ATTACKING U.S. INFRASTRUCTURE.

geted BBC and VOA broadcasts on the Hot Bird 6 commercial satellite, but when the broadcasts were moved to transmit through other commercial satellites, the jamming targeted those satellites as well.[294] In the same year, the head of the Islamic Republic of Iran Broadcasting publicly acknowledged that the Iranian government engaged in the jamming of foreign broadcast satellites.[295]

Al Jazeera faced targeted attacks in January 2012 after its coverage of the conflict in Syria. The origin of the attacks was traced to two locations in Iran.[296] Later that year, Iran was supported by the Syrian government in a coordinated jamming effort against approximately 25 international broadcasters, "including the BBC, France 24, Deutsche Welle and the Voice of America."[297] A similar report in July of 2019 stated Iran International, a London-based TV station, believed its signals were being blocked via uplink jamming originating from Iran.[298]

Iran has publicly claimed the ability to spoof GPS receivers. In 2011, Iran claimed to have forced a U.S. RQ-170 drone to land inside its borders by jamming its satellite communications links and spoofing the GPS receiver. An Iranian engineer was quoted at the time as saying that the drone landed "where we wanted it to, without having to crack the remote-control signals and communications."[299] Though a former Pentagon spokesperson claimed there was "no indication the drone was brought down by hostile activity of any kind," President Obama did acknowledge that Iran had possession of the drone.[300] If Iran's claims of electronic jamming are true, they represent a significant counterspace capability that could be used to thwart U.S. precision-guided weapons and aircraft in the future.

In 2019, there were similar reports of GPS spoofing of commercial U.S. ships in the Gulf of Oman. Several ships reported a loss of GPS signal and were captured in Iranian territorial waters. After 11 reported incidents, the U.S. Maritime Administration issued a warning to U.S. vessels to be aware of GPS interference in the area.[301] The advisory warned of Iranian GPS jammers operating on an island near the Strait of Hormuz with the goal of causing ships and aircraft to "inadvertently wander into Iranian waters or airspace in order to justify a seizure." The warning also mentioned instances of "spoofed" communications from ships claiming to be U.S. or other countries' warships. [302] Similar GPS interference was reported by British ships, prompting British media reports that intelligence services were concerned that Iran had used Russian GPS spoofing technology to guide the vessels into Iranian waters.[303] In 2019, numerous oil tankers from varying regions reported seizures in the Strait of Hormuz, followed by an Iranian shoot-down of a remotely piloted U.S. Navy aircraft over the international waters in the region.[304]

Also in 2019, the commander-in-chief of the Islamic Revolutionary Guard Corps (IRGC) announced the creation of a new mounted hardware unit called *Sepehr 110* to protect its systems from electronic warfare.[305] State media credits the system as being developed by IRGC experts and "invulnerable to hacks, eavesdropping, radio jamming, and electromagnetic disturbance" but there has been no external verification of the system.[306]

Later that year, the Research and Self-Sufficiency Jihad Organization of the Iranian army unveiled a portable jamming system attachable to vehicles and reportedly capable of detecting and disrupting drone flights.[307] These announced upgrades of counterdrone capabilities, including a system capable of participating in electronic warfare and radar evasion, have not been corroborated outside of state-sponsored media.[308]

Cyber

Iran began developing its cyber capabilities through independent hackers who gained notoriety in the early 2000s. The Iranian government often encourages its hackers through recruiting into its own cyber forces or supporting independent operations against its enemies, representing a somewhat unique approach.[309] Though initially modest, Iranian cyber capabilities have grown significantly in the last decade, becoming "notable players" in the cyber realm.[310] Iran has devel-

oped advanced offensive cyber capabilities that could potentially target U.S. space systems in the future. With three separate branches of the Iranian military contributing to cyber infrastructure, Iran claims over 100,000 cyberwar volunteers and recently established a Joint Chiefs of Staff Cyber Command to better organize its efforts.[311]

This increase in cyber activity has been mirrored in the country's budget; in 2017, the budget of the National Center for Cyberspace reportedly increased by 45 percent in one year, swelling to $1.2 million. [312] Iranian willingness to employ cyberattacks against targeted defense companies, media conglomerates, and adversaries also appears to be increasing.[313]

Iran has demonstrated its cyber capabilities by attacking U.S. infrastructure, though it has often targeted private companies as opposed to government systems. In 2012, Iran launched a distributed denial of service (DDOS) attack against U.S. banks and telecommunications companies, which resulted in monetary losses in the millions.[314] This particular incident prompted a public statement by then-Secretary of Defense Leon Panetta warning that the imminent threat of a cyberattack that could cause significant property damage or kill U.S. citizens would be sufficient justification for a pre-emptive military strike.[315] In 2019, the FBI was made aware of attempts, likely originating from Iran, to gain access to the systems of U.S. satellite technology companies.[316]

Various malware programs, including the destructive Shamoon virus with the ability to fully wipe computer systems, have been tied to Iranian state-sponsored hacking groups. The director of the U.S. Cybersecurity and Infrastructure Security Agency issued a warning describing a similar type of destruction, citing a "rise in malicious cyber activity" from Iranian actors. [317] As tensions rise worldwide with Iran, so do hacking attempts. In a 48-hour time period in January 2020, attacks from Iranian IP addresses were recorded at up to 500 million attempts per day globally.[318] Although there are few confirmed instances of Iran using cyberattacks against space systems, Iran's increasingly sophisticated cyber capabilities suggest that it could employ such attacks on space systems if needed.

SUMMARY

Iran is still far from developing direct-ascent ASAT weapons, even with its increased focus on launch vehicle development and continued development of ballistic missile capabilities. Similarly, with only four successful satellites that have reached orbit and a growing string of failed launches, Iran is unlikely to develop a co-orbital ASAT capability in the near future. To make significant progress on kinetic and non-kinetic counterspace systems, Iran would likely need to acquire technology and resources from a major counterspace actor, such as Russia or China. However, Iran has growing electronic and cyber counterspace capabilities and continues to demonstrate successful jamming and hacking attacks against foreign governments and civilian systems.

Number of Successful Orbital Launches in 2019[319]

0

NORTH KOREA

"North Korea has been building new missiles, new capabilities, new weapons as fast as anybody on the planet,"

GENERAL JOHN E. HYTEN
VICE CHAIRMAN OF THE JOINT CHIEFS OF STAFF, UNITED STATES AIR FORCE[320]

NORTH KOREA SUCCESSFULLY ORBITED ITS FIRST SATELLITE in December 2012 after three failed attempts in July 2006, April 2009, and April 2012. Its fifth attempt, in February 2016, successfully placed a second satellite in orbit. Both successful orbital launches from North Korea have been on the *Unha-3* SLV, whose militarized adaptation is likely the same vehicle outfitted with a reentry vehicle in place of an orbital satellite.[321] Like many other spacefaring nations around the globe, North Korea's space capabilities are closely tied to its ballistic missile development.

A North Korean law journal referenced the close relationship between space capabilities and ballistic missiles, stating "it is an undeniable truth that satellites launched into orbit by many countries around the world were made possible by rocket propulsion." While defending the country's satellite launching program, the article continued to state that the main difference between a peaceful space launch and a ballistic missile is whether the launch vehicle is furnished "with a satellite or a bomb."[322]

Although reaching orbit is a significant achievement, many experts doubt that the two successfully launched satellites perform all of the functions the North Korean government claims.[323] In a 2016 interview with the Associated Press, the head of the North Korean space agency stated his intent

Satellite Imagery of the Sohae Satellite Launching Ground After a Test on December 7, 2019. Differences include scarred vegetation and the moving of equipment. The facility hosted rocket engine tests on December 7 and December 13, 2019.

PLANET / BEYOND PARALLEL

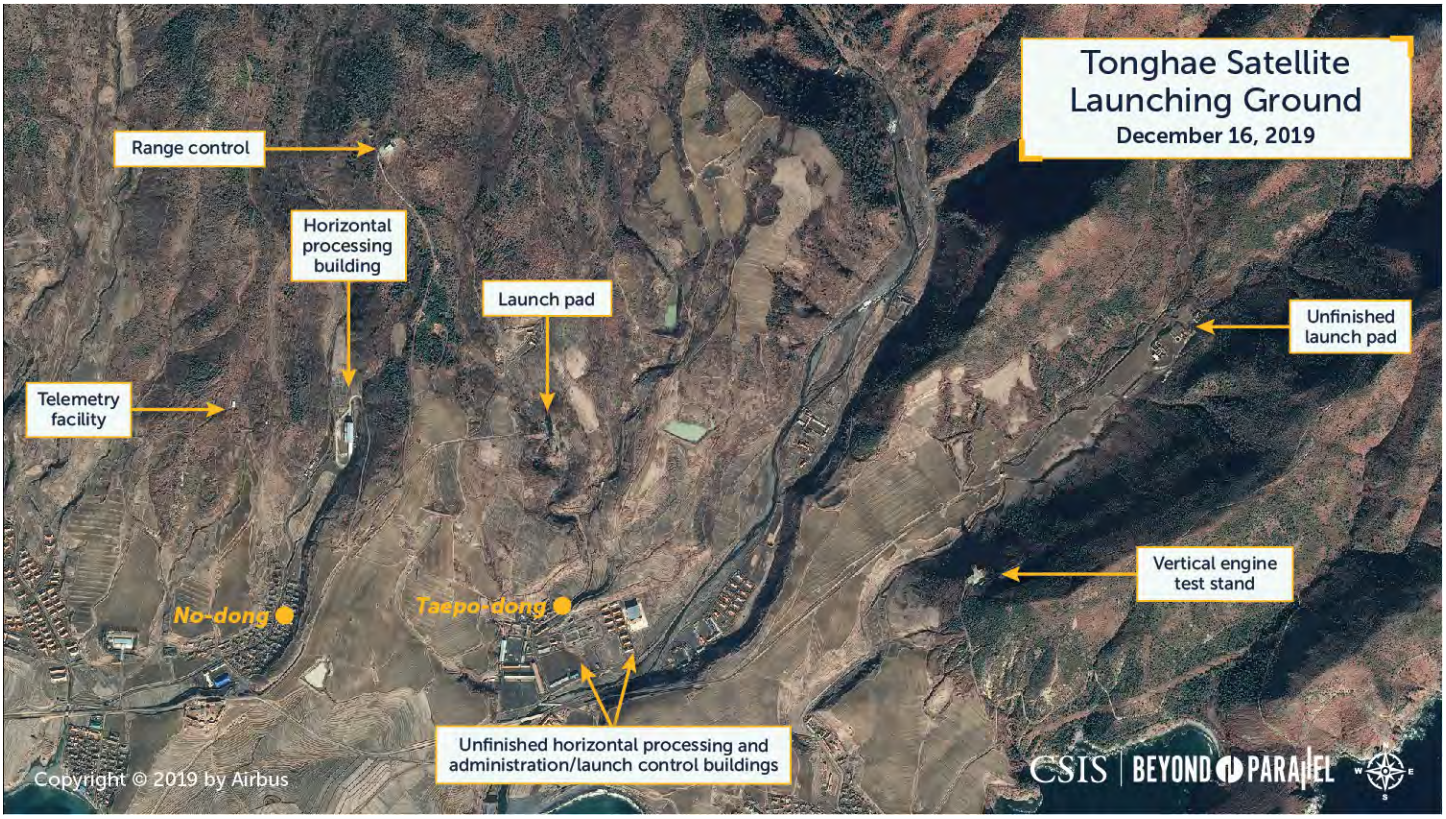
to continue launching Earth observation satellites, and his aspirations to send a mission to the moon around 2026. He was quoted as saying, "Even though the U.S. and its allies try to block our space development, our aerospace scientists will conquer space and definitely plant the flag of the DPRK on the moon."[324]

There is little indication that North Korea is making substantial efforts to build or sustain a space industrial base, but its missile program is advancing. There were 11 separate North Korean missile tests in 2019 alone, which involved as many as 20 rockets in total.[325] Additional satellite footage taken in early 2020 showed increased activity at a known missile launch site, possibly signaling more tests in the near future.[326]

Space Launch Facilities

NORTH KOREA HAS TWO ESTABLISHED LAUNCHING AREAS for space capabilities: the Tonghae Satellite Launching Ground and the Sohae Satellite Launching Ground. The Tonghae Satellite Launching Ground is North Korea's oldest ballistic missile and space launch facility, although a successful orbital launch has never been achieved at the facility. According to December 2019 satellite imagery, there was increased activity at the site, including a group of people and possibly crates, but no sign of major renovations that would have to take place to prepare the facility for a vehicle test. However, North Korea has used mobile launching platforms for all recent land-based ballistic missile tests, which could be conducted in the grounds of Tonghae.[327]

The Sohae Satellite Launching Ground showed initial steps of disassembly in satellite imagery in the summer of 2018, but reassembly began again after U.S - North Korea Summits in Singapore and Hanoi.[328] In late 2019, North Korea conducted two engine tests at the Sohae Satellite Launching ground, believed to be modified liquid-fueled engines for long-range missiles.[329] While the specifics of the tests were unconfirmed, KCNA state media referred to the successful tests as "defence science achievements" that will "have an important effect on changing the strategic position" for the country.[330] Although conducted at a satellite launching pad, experts assess that it was likely another missile test or a step towards ICBM development, rather than a space vehicle launch.[331]



Satellite Imagery of the Tonghae Satellite Launching Ground on December 16, 2019. Analysis shows one launch pad, a second unfinished launch pad, and missile storage for the *No-dong* medium range ballistic missile, and *Taepo-dong* SLV. Both noted missiles are capable of reaching LEO.

AIRBUS / BEYOND PARALLEL

SPACE ORGANIZATION AND DOCTRINE

North Korea keeps its doctrine and operational concepts largely under wraps, including what is released about its counterspace capabilities. The absence of discussion about counterspace capabilities that could threaten the U.S. military is unusual given the aggressive rhetoric used by the regime in touting its nuclear and missile programs.[332] The country continues to advocate internationally for its right to a sovereign space program.[333]

When the regime has spoken about its space program at the United Nations, delegates speak of respect of international norms to maintain peaceful development and use of outer space, including the North Korean space program's right to help the country grow economically.[334] In March 2009, North Korea became a signatory to two major UN space treaties: the Outer Space Treaty of 1967 and the Convention on Registration of Objects Launched into Outer Space of 1974.[335] Four years later, in April 2013, the country's Supreme People's Assembly established the National Aerospace Development Administration (NADA), the official North Korean space agency.[336] Additionally, space has often been included in five-year plans that the regime has put forward.[337]

In October 2017, a delegate to the United Nations was reported in state media as saying "peaceful development of outer space is actively conducted in accordance with the 2016-2020 plan for national outer space development."[338] As reported, this plan included an aim to launch a geostationary satellite—a much more challenging feat which would require a more powerful launch vehicle.[339] State media reported a successful ground test of a new launch vehicle for this purpose, but it has not noted any attempts at an actual launch.[340] The regime hopes to use satellites to monitor crop and forestry growth as well as to improve communication ca-

pabilities.[341] The plan expressed a goal to field a satellite communication system by 2019, though there is no indication that goal was achieved.[342]

COUNTERSPACE WEAPONS

Kinetic Physical

Current space launch vehicles and ballistic missiles demonstrated by North Korea could serve as the basis for a kinetic ASAT capability, but many technological hurdles remain. To date, North Korea has not tested, or indicated that it is attempting to develop, a direct-ascent or co-orbital ASAT capability. It is unlikely that North Korea could quickly gain the technology for an effective direct-ascent or co-orbital ASAT weapon, as it has only succeeded in placing two satellites into orbit, the operation of which are not confirmed outside state media. This additional capability would also require onboard sensors (e.g., optical, infrared, radar) and a guidance system to steer the weapon into a target satellite.

It is conceivable that North Korea could field a crude direct-ascent ASAT capability in the near term in the form of an adapted ballistic missile. This would be possible with the launch of an unguided warhead set to detonate in the vicinity of a target satellite. Rather than directly strike a satellite, it could create a debris field that would complicate future operations for satellites in a similar orbit. For example, the North Korean *No Dong-1* medium-range ballistic missile would likely be able to carry a 1200 kg payload to a maximum altitude of 600 to 750 km—well within the LEO regime.[343] Missiles launched from North Korean territory could more easily be used in a conventional attack on nearby ground stations that support satellite operations, such as the U.S.-operated GPS monitoring station in South Korea and other ground stations as far away as Guam.[344]

Non-Kinetic Physical

The technology necessary to develop directed energy weapons, such as lasers that are able to dazzle or blind the sensors on satellites, requires a level of sophistication that North Korea likely does not possess.[345] It is possible, however, that North Korea could develop a crude EMP weapon for use against space assets. In 2017, North Korea successfully tested a hydrogen bomb underground, a claim that was confirmed by South Korea and Japan.[346] Officials from Pyongyang released a photo of the hydrogen bomb and asserted that the bomb is able to fit on an ICBM.[347] Kim Jong-un has called for further improvements in nuclear bombs similar to this test in the "Songun" spirit, which places the military first.[348] In January 2020, KCNA reported that Kim Jong-un declared the world would soon see a new strategic weapon, adding that there will never be denuclearization on the Korean peninsula.[349]

A nuclear weapon on a long range missile would theoretically give North Korea the capability to create a high-altitude EMP effect.[350] In 2018, The Daily NK—a South Korean news site—obtained North Korean internal propaganda documents aimed to inform citizens that the country has the capability to damage enemies' military and civilian electronic systems beyond repair as a result of a nuclear EMP attack.[351] North Korea is not a signatory of the 1963 Partial Test Ban Treaty, and the country has not tested a nuclear weapon at high altitudes.[352]

Electronic

North Korea has acquired and is constantly using electronic forms of attack against varying space systems. In 2010, South Korean Defense Minister Kim Tae-young said in a speech to parliament that "North Korea has imported vehicle-mountable devices capable of jamming GPS signals from Russia." These downlink jamming systems reportedly have an effective radius of 50 to 100 km. North Korea began using this jamming equipment against

NORTH KOREA HAS BEEN CARRYING OUT CYBERATTACKS BY PLACING INDIVIDUALS IN SCATTERED FOREIGN COUNTRIES IN AN ATTEMPT TO DISGUISE THE ORIGIN OF THE ATTACKS.

South Korea in August 2010, but South Korean forces could not pinpoint the location of the jammers at that time because the jamming lasted just 10 minutes in each instance.[353]

In the decade since, North Korea has repeatedly used its GPS jamming capabilities against South Korea. More GPS jamming occurred in December 2010 and again in March 2011, which coincided with a U.S.-South Korean military exercise. Jamming occurred again in April 2012, disrupting air traffic at Incheon and Gimpo international airports, forcing flights to use alternative navigation systems.[354] In March and April 2016, over 250 South Korean fishing boats lost access to GPS, forcing them to return to shore.[355] A few days later, South Korea complained to the UN Security Council that North Korea was jamming GPS signals across the border, with the jamming coming from five areas in North Korea: Pyongyang, Kaesong, Haeju, Yonan county, and Mount Kumgang.[356] Documents state that in 2016, 2,143 aircraft disclosed GPS interference, likely due to North Korean jamming operations.[357]

The South Korean Defense Ministry has said it believes the jamming attacks originate from "a regiment-sized electronic warfare unit near the North Korean capital Pyongyang, and battalion-sized units closer to the inter-Korean border."[358] The jammers are mounted on mobile platforms and are operated intermittently, which could be difficult to locate and neutralize in a conflict. North Korea appears to be gaining operational experience using these systems in peacetime. Because the GPS jammers were acquired from Russia, it is possible that North Korea could also have acquired other types of jamming capabilities that can target different satellite systems, such as uplink jammers that can disrupt military satellite communications.

Additionally, AIS spoofing has been used in shipping vessels during 2019 likely in an attempt to hide what is assumed to be coal smuggling operations. A report details the suspicious behavior of one of North Korea's largest bulk ships, the *Tae Yang,* which North Korea relies on for imported goods and revenue. The *Tae Yang* consistently broadcasted a unique identification number assigned to another vessel to disguise its own illicit movements, while still transmitting AIS data. Another report by the UN Panel of Experts has uncovered additional examples of AIS spoofing techniques used by North Korean ships to avoid sanctions.[359]

According to minutes from a 2008 meeting about network surveillance capabilities, North Korean officials inquired about a satellite jamming system to two groups of internationally contracted engineers. The meeting ended with an agreement that "the number of jamming systems that prevents interception by satellite should be increased." However, analysts believe it is possible that the inquiry was an excuse to get imported German cellular detection equipment, which was subsequently used to catch North Korean citizens with Chinese cell phones.[360]

Cyber

Under the Kim Jong-un regime, North Korea has used its cyber forces frequently, first launching attacks on South Korea and the United States, then branching out to others. According to CrowdStrike, North Korean hackers have the second-fastest breakout time (the time needed for hackers to achieve their objectives in an attack) of any hacking organization in the world, behind Russia. North Korea's malicious cyber activity tends to focus on financial targets or inter-Korea issues. A majority of the cyberattacks stemming from North Korea are "linked to currency generation and economy-bolstering efforts for the Kim regime."[361]

Experts believe there are around 6,000 - 7,500 military personnel conducting cyber warfare for the North Korean state. Cybersecurity defector and founder of North Korea Intellectuals Solidarity, Kim Hueng-kwang, said most cyber operations in the country are organized in a unit directly under North Korea's main overseas intelligence agency, the Reconnaissance General Bureau (RGB).[362] He emphasized that North Korea was "inspired by the Chinese cyberwar units and learned from them."[363] According to Kim,

members of an elite North Korean hacking group go on covert missions overseas, generally to places with better internet than the notoriously shielded country, to lower the risk of being caught. South Korea's vice foreign minister confirmed this report, telling Reuters that North Korea has been carrying out cyberattacks by placing individuals in scattered foreign countries in an attempt to disguise the origin of the attacks. [364]

A leaked report sent to the UN Security Council's North Korea sanctions committee stated that through 35 separate cyberattacks, North Korea has stolen over $2 billion, which has likely been used to fund weapons development.[365] Subsequently, the U.S. Department of the Treasury announced sanctions for three state-sponsored cyber groups from the country, naming them responsible for malicious cyber activity on critical infrastructure.[366]

North Korean hackers have also been tied to a nuclear power plant in India and possibly the Indian Space Research Organization during its Chandrayaan-2 mission, although Indian space authorities deny they were compromised. [367] They are also suspected to have hacked an Israeli aerospace and defense company.[368] Given its demonstrated cyber capabilities, it is conceivable that North Korea could initiate a cyberattack against U.S. space systems or ground stations, although there is no publicly available information to suggest this has happened to date.

SUMMARY

North Korea has demonstrated growing capabilities in two counterspace weapons categories: electronic and cyber. It is also developing some of the necessary technologies to field a non-kinetic physical nuclear EMP counterspace weapon through its nuclear program, but this does not appear to be the intent of those activities.

Although North Korea has demonstrated its dedication to increasing the range of its ICBM-class missiles, its limited number of successful orbital launches suggest that the country is far from developing the capabilities needed to pose a significant kinetic physical threat to foreign satellite systems. The only significant risk of non-kinetic physical attack from North Korea is high altitude nuclear detonation, a devastating, irreversible counterspace attack that would indiscriminately affect systems in the target satellite's orbital regime. Importantly, North Korea is improving its electronic warfare capabilities, as demonstrated in continued GPS jamming and spoofing operations, and is continuing to use cyberattacks against a variety of targets worldwide.

Number of Successful Orbital Launches in 2019[369]

6

INDIA

"When India celebrates [its] 75th year of Independence in 2022, and if possible even before, an Indian son or daughter will undertake a manned space mission on board 'Gaganyaan' carrying the national flag."

PRIME MINISTER NARENDRA MODI[370]

INDIA JOINED THE WORLD STAGE AS A RISING SPACE POWER by launching its first satellite from the Satish Dhawan Space Center in 1980. India has since developed highly successful launch vehicles, a range of communications, imaging, and other critical satellites, and is beginning serious development of counterspace capabilities. While India has no overarching national space policy yet, the government of India is in the process of creating one.[371] Currently, it does have various organizations dedicated to the space domain in both the military and civil sectors, each with supporting policies and doctrine. Among these organizations is the principal space organization in India, the Indian Space Research Organization (ISRO), which is responsible for maintaining the SLVs and spaceports of India.

Currently, India has two operational orbital launch vehicles, the Polar Satellite Launch Vehicle (PSLV) and the Geosynchronous Satellite Launch Vehicle (GSLV). These two vehicles launched six times in 2019, representing only a small portion of the 67 total Indian launches since 1980 from the Satish Dhawan Space Centre.[372] India made history in 2017 with the largest number of satellites on any single mission, launching 104 satellites with one PSLV, breaking the previous record of 37 satellites held by Russia since 2014. All but three of these satellites were foreign owned.[373]

INDIA

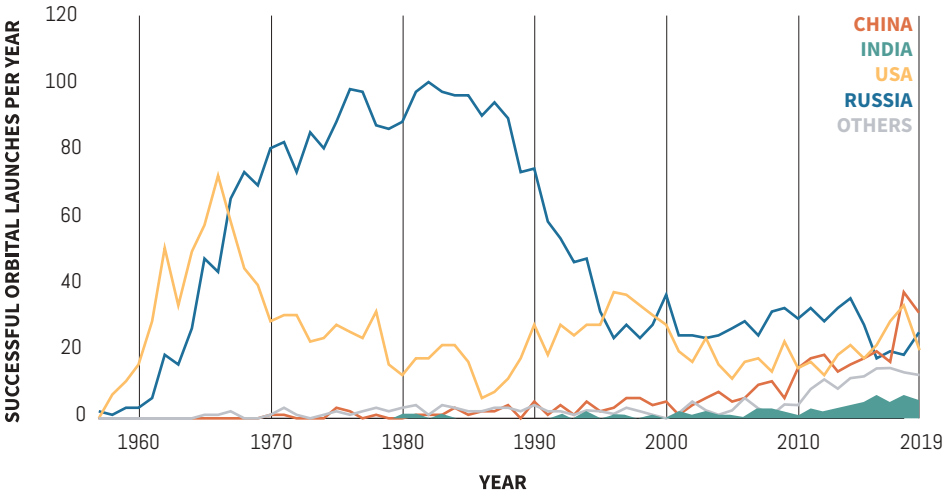


Figure 12: Indian Orbital Space Launches (1957 - 2019).

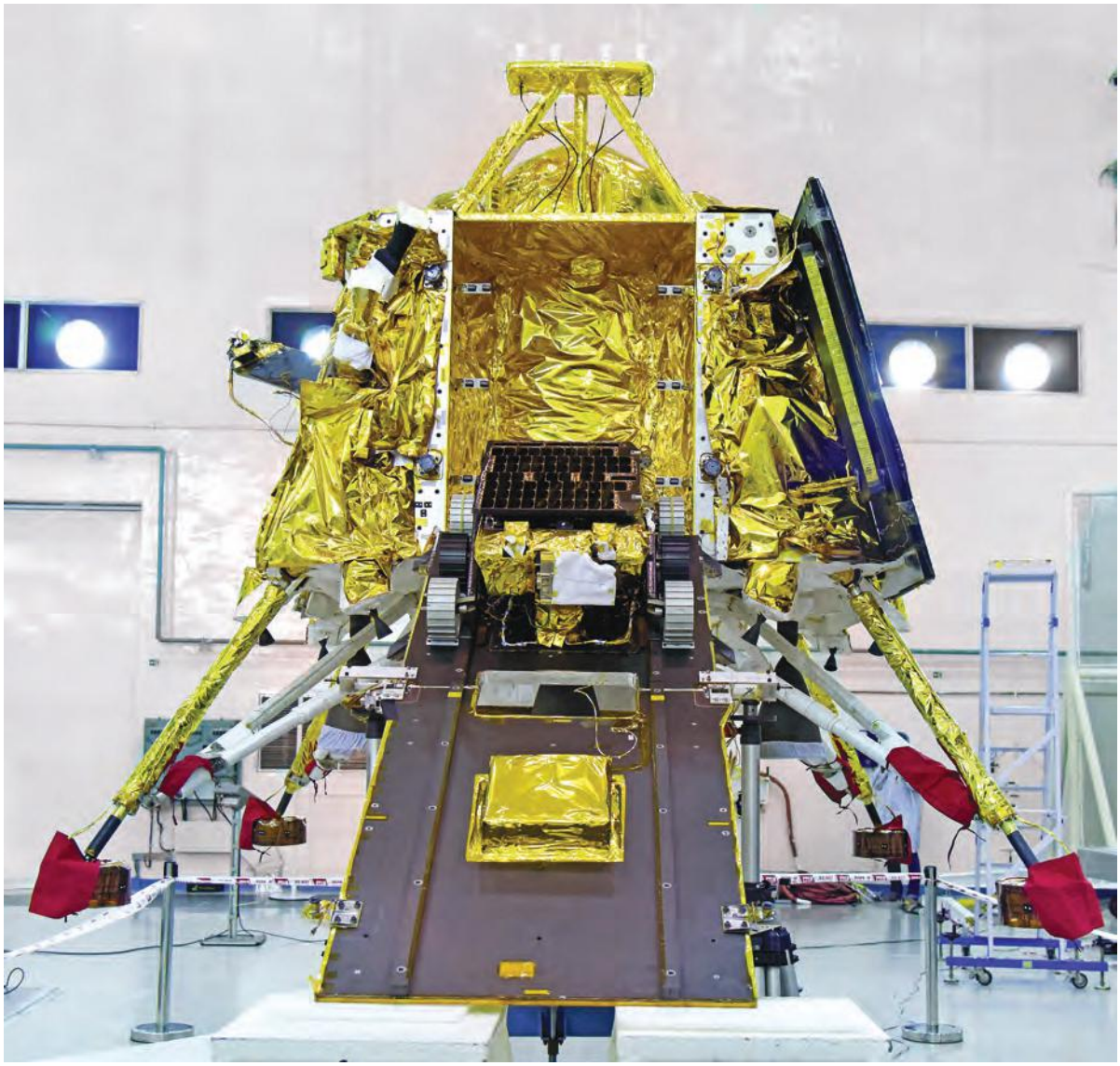
SPACETRACK.ORG / CSIS AEROSPACE SECURITY[374]

The Satish Dhawan Space Center has been India's only major spaceport since it began launching in 1980. However, due to the anticipated increase in demand for national and commercial space launch in the coming years, the Indian government has begun the land acquisition process for the construction of a new spaceport.[375] The proposed spaceport, to be located in the southern state of Tamil Nadu, is planned to mainly service India's newest launch vehicle, the Small Satellite Launch Vehicle (SSLV).[376] A derivative of the PSLV, this new Indian launch vehicle is rated to carry "up to 500 kilograms to mid-inclination low Earth orbits and 300 kilograms to [sun-synchronous orbit (SSO)]."[377] The location of the proposed spaceport will allow for launching southward into a polar or near-polar orbit, which is difficult from the Satish Dhawan Space Center due to the need to maneuver around Sri Lanka.

Only three countries—China, the Soviet Union, and the United States—have ever "soft-landed" on the lunar surface.[378] In 2009, India successfully launched the *Chandrayaan-1* spacecraft, which was designed to orbit the moon and conduct a hard-landing for the purpose of targeting and practicing a future soft-landing.[379] In 2019, the *Chandrayaan-2* spacecraft was placed on a GSLV and launched into lunar orbit. While on approach to the lunar surface to attempt a soft-landing, the Vikram Lander lost contact with the ISRO and crashed into the lunar surface.[380] After about a month of attempting to re-establish contact with the lunar lander, the Indian government made an official announcement that they had lost contact and were unable to recover the spacecraft.[381] However, this failure has only reinvigorated the Indian space program and public.

In an announcement on January 1, 2020, Chief Kailasavadivoo Sivan, head of the ISRO, stated that the top priorities for the ISRO in 2020 are a *Chandrayaan-3* mission to the lunar surface and the *Gaganyaan* human spaceflight program, though it is unlikely that either will launch before 2021.[382] The *Chandrayaan-3* mission will similarly attempt to conduct a soft-landing on the lunar surface. When asked if a crewed mission to the moon was in the near future for India, Sivan said, "definitely, but not im-

THE TOP PRIORITIES FOR THE ISRO IN 2020 ARE A CHANDRAYAAN-3 MISSION TO THE LUNAR SURFACE AND THE GAGANYAAN HUMAN SPACEFLIGHT PROGRAM, THOUGH IT IS UNLIKELY THAT EITHER WILL LAUNCH BEFORE 2021.



Vikram Lander and Pragyan Rover. The Vikram lander was launched on the *Chandrayaan-2* mission, but it did not achieve a successful soft landing on the lunar surface.

ISRO

mediately."[383] Four Indian astronauts will be sent to Russia for 11 months to receive training in preparation for the *Gaganyaan* program. Additional program-specific training will also take place in India.[384]

ORGANIZATION AND DOCTRINE

India does not have an official military department focused on space. It instead created a separate agency, the Defence Space Agency (DSA), to coordinate between and command the space assets of the Indian Army, Navy, and Air Force, including India's new direct-ascent ASAT capabilities.[385] According to the two-star general appointed to head the DSA, "the agency will eventually grow into a full-fledged Space Command in the years ahead."[386] To date, however, there is no confirmed timeline for this growth. Within the DSA, India established the Defence Space Research Organization (DSRO) in late 2019 to further develop and test counterspace systems and related technologies.[387]

In late July 2019, India's top strategic planners from several agencies gathered to begin to establish new policies and doctrine for future military and non-military uses for space. Called IndSpaceEx, the strategic planners were led through a wargaming simulation that was meant to assess military assets of other leading space powers—namely the United States, China, and Russia—to better assess the level to which India must counter international space threats.[388] The session's conclusion was that future wars may be dominated by activities in the cyber and space domains,

leading to asymmetric advantages or disadvantages.[389]

A 2019-2020 annual report released by the Government of India's Department of Space detailed initial steps of an official space policy for the country. This policy will "support the pursuance of space activities by various agencies in India including private sector and start-up companies in the aerospace sector."[390] It is clear through India's military space reorganization, renewed focus on commercial partners, and it's test of a direct-ascent ASAT in March 2019 that the Indian leadership views space as a key operational domain.

COUNTERSPACE WEAPONS

Kinetic Physical

The Indian government took notice of China's successful 2007 direct-ascent ASAT, causing it to shift focus to protecting its vulnerable space assets from a Chinese threat. As one scholar noted, "It suddenly reminded them that their diverse space assets were now at risk,

Mission Shakti

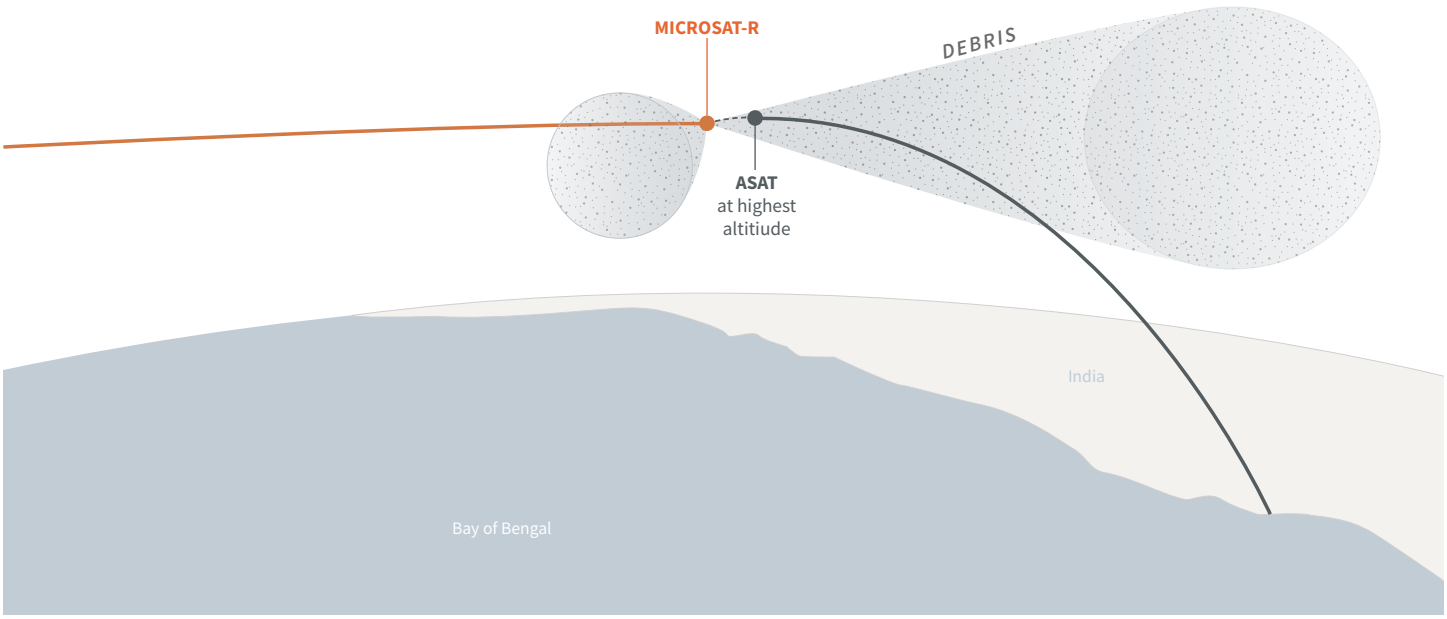
ON MARCH 27, 2019, India successfully launched a Prithvi Delivery Vehicle Mark-II (PDV MK-II) missile defense interceptor at one of its own satellites. Launched in late January 2019, the target satellite, *Microsat-R*, was specifically placed in a low-altitude sun-synchronous orbit as the target for an ASAT test. After the successful test in March, independent analysts realized that an earlier attempt to intercept the satellite on February 12 of the same year failed.[391]

What was perhaps most notable about the Indian ASAT test was the muted international outcry that occurred afterward. This was likely due in part to the minimal amount of orbital debris created—only about 400 pieces remained in orbit immediately after the test, compared to the over 3,000 pieces of debris created during the 2007 Chinese ASAT test. The Indian ASAT test took place at a relatively low altitude, and at the time of impact, the interceptor was on a downward trajectory. This resulted in much of the debris having a downward trajectory, allowing it to be more quickly deorbited. Given these factors, it is likely that the Indian government was attempting to limit the potential for long-lasting orbital debris.[392] Since the test, a majority of the debris has deorbited, and by the end 2019, just 18 pieces of debris large enough to track remained in orbit.[393]

The Indian ASAT test did not receive the same level of international outcry as the Chinese ASAT test, in part because it produced much less orbital debris. The United States, for example, only had one government official speak out against the test. NASA Administrator Jim Bridenstine decried the test because some pieces of debris were pushed to a higher altitude, threatening the astronauts on the International Space Station.[394] While public international outcry was minimal, Pakistan was one of few states to openly denounce the test, urging all countries to "condemn India's action and strengthen international laws regarding the militarization of space."[395] Additionally, the Union of Concerned Scientists denounced the test, expressing that this test harmed international efforts to prevent further weaponization of outer space.[396]

Figure 13: Depiction of Kinetic Physical ASAT Test by India in 2019. Muted international outcry in response to this ASAT test was, in part, due to the low amount of debris created because of the slight downward trajectory of the missile on impact.

AEROSPACE SECURITY PROJECT / EMILY TIEMEYER



hostage to the dangers emanating from their most formidable regional threat." For years, defense planners debated the merits of conducting a similar kinetic ASAT test to signal to China and other nations that India had the ability to retaliate in kind if its space assets were attacked.[397] The government eventually concluded that India should pursue kinetic ASAT weapons.

On March 27, 2019, India became the fourth country—behind the United States, China, and Russia—to successfully test a direct-ascent ASAT missile. Named Mission Shakti, meaning "strength" in Hindi, the test was conducted with an Indian-produced ballistic missile which intercepted a small target satellite in LEO.[398] In a tweet, Prime Minister Narendra Modi said this test will "have a historic impact on generations to come."[399]

"In the journey of every nation there are moments that bring utmost pride and have a historic impact on generations to come."

PRIME MINISTER NARENDRA MODI[400]

India does not have any publicly known co-orbital ASAT capabilities. However, Defence Research and Development Organization Chief G. Satheesh Reddy announced in April 2019—less than a month after the success of Mission Shakti—that India was developing co-orbital ASAT capabilities and that the details remained classified.[401] India is developing, in partnership with France, the technical capabilities to conduct RPO on orbit as part of its efforts to develop a national space station.[402] RPO proficiency is a key step toward the fundamental capabilities of building some types of co-orbital counterspace weapons.

The Indian military also has the ability to directly attack satellite ground stations. Indian special operations units are specially trained to "to carry out crippling attacks against critical enemy targets miles away."[403] The newly created Armed Forces Special Operations Division is designed and modeled off of the United States Joint Special Operations Command (JSOC).[404]

Non-Kinetic Physical

Thus far, India does not appear to have developed and tested non-kinetic physical counterspace weapons. However, the 2010 *Technology Perspective and Roadmap* released by the Ministry of Defense detailed that ASAT weapons "for electronic or physical destruction of satellites (2,000 km altitude above earth's surface) and geosynchronous orbits" are a key area of future focus.[405] Following this, a new *Technology Perspective and Capability Roadmap* in 2013 noted a focus on developments in electronic weapons, specifically miniaturization of EW elements as payloads on satellites.[406]

PDV-MK II Missile Lifting Off on Track to Intercept *Microsat-R* on March 27, 2019. The missile used by India during its first ASAT test was an indigenously manufactured missile.[409]

GOVERNMENT OF INDIA

In its 2018 *Technology Perspective and Capability Roadmap*, India detailed investments in a two-phase Tactical High Energy Laser System. The second phase of this system is intended to play an "anti-satellite role from ground & aerial platform."[407] Following the Mission Shakti test, DRDO Chief Satheesh Reddy stated that India was in the process of developing different ASAT technologies, including directed-energy weapons, lasers, and electromagnetic pulses.[408] However, beyond these general statements and reports, the government of India has not divulged any details of these activities.

As a nuclear-armed state, India has the ability to launch a nuclear warhead into space as a counterspace weapon. Theoretically, in addition to the kinetic properties of the nuclear weapon, India could use the EMP effect from a high-altitude nuclear detonation to disable satellites. However, there is no publicly available indication that India is pursuing a nuclear EMP space weapon.

Electronic

India's 2018 *Technology Perspective and Capability Roadmap* also shows investment in an integrated EW system with requirements to "detect, monitor, locate and jam enemy cellular receivers and satellite communication receivers."[411] Another planned system has similar requirements as the integrated system and is intended to also be able to "carry out jamming & spoofing of satellite based positioning systems."[412] However, India has not yet publicly demonstrated its jamming or spoofing capabilities.

Cyber

In 2019, the government of India set up the Defence Cyber Agency (DCA). Similar to the Defence Space Agency, the DCA is meant "to control and coordinate joint cyber operations."[413] There have been questions as to whether India may have some kind of cyber deterrence against enemy satellites with both space- and land-based systems; however, Union Minister Shripad Naik has stated that such information is sensitive and therefore is unable to be confirmed or denied.[414]

"India has always been opposed to the weaponization of space and an arms race in outer space, and this test does not in any way change this position."

PRIME MINISTER NARENDRA MODI [410]

SUMMARY

Although India has had a recent successful direct-ascent ASAT test, other types of counterspace weapons are far from developed. As India focuses more on building out its space assets, as well as its counterspace assets, subsequent counterspace weapons tests may occur. While the 2019 ASAT test has certainly caused great debate in the international space community, the muted official international response sets a different precedence from the Chinese 2007 test. With little to no repercussions, India demonstrated that a lower-altitude ASAT test may be accepted by the international community.

Number of Successful Orbital Launches in 2019[415]

13

OTHERS

"I'm convinced that in the future, if we were to get into a conflict with a peer or near-peer competitor, we're going to have to fight for space superiority."

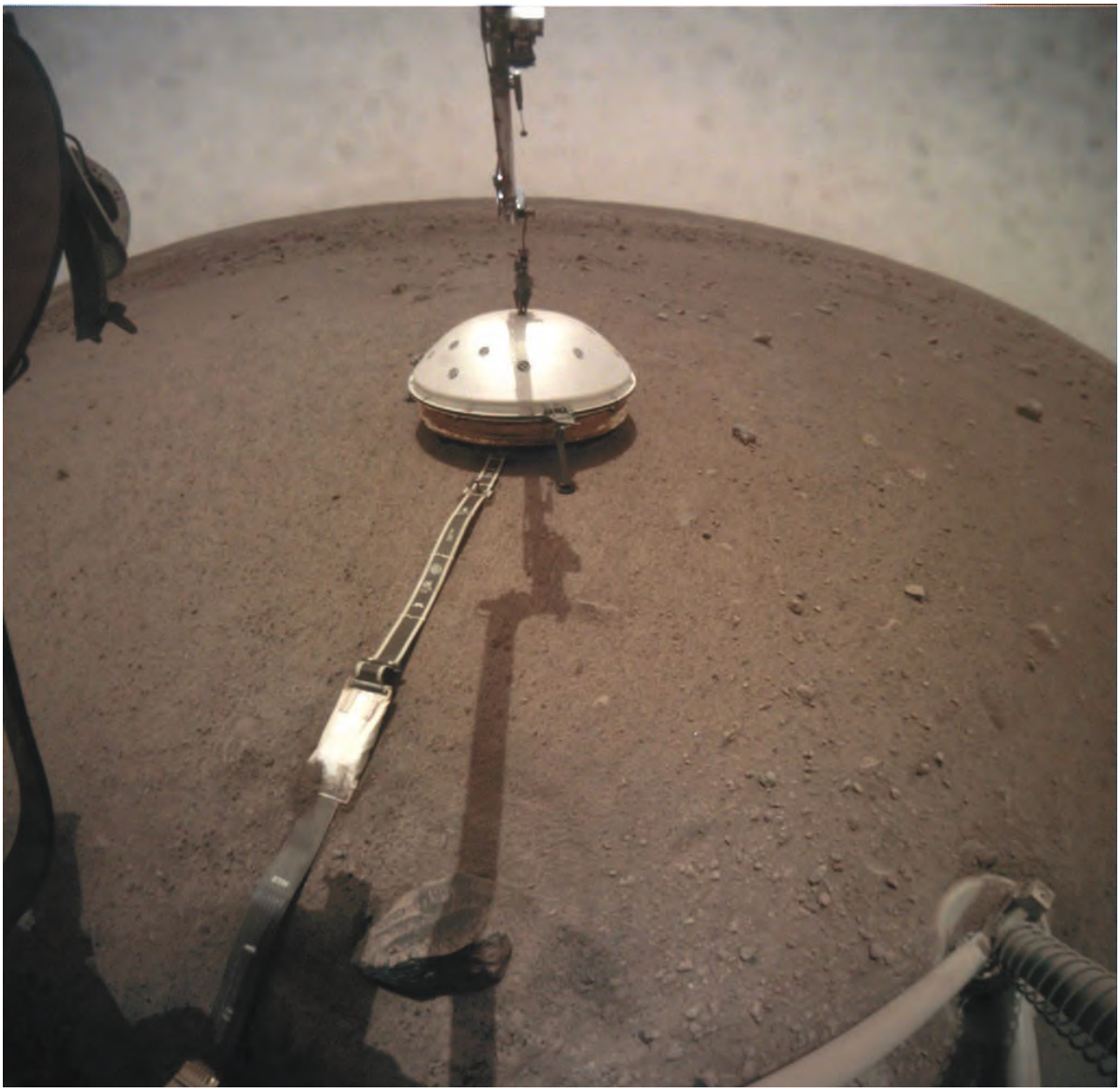
GENERAL JOHN RAYMOND, CHIEF OF SPACE OPERATIONS AND COMMANDER OF U.S. SPACE COMMAND[416]

WHILE THE PREVIOUS CHAPTERS HAVE BEEN DEDICATED to the countries making the largest strides in counterspace capabilities—China, Russia, Iran, North Korea, and India—they are not the only ones thinking strategically about the changing space environment. This chapter includes significant discussion and developments related to counterspace capabilities in other countries and non-state actors.

FRANCE

AS THE THIRD OLDEST SPACE PROGRAM IN THE WORLD, France has accomplished much since it first established its national space agency, the Centre national d'études spatiales (CNES), in 1961. France launched its first satellite in 1965, led the development of the Ariane family of launch vehicles, and became one of the foremost European space powers through its strong relationship with the European Space Agency (ESA).[417]

In 2018, the CNES was a key partner of NASA's Mars Discovery Program, providing the InSight (Interior Exploration using Seismic Investigations, Geodesy and Heat Transport) mission. InSight deployed a seismometer, named SEIS (Seismic Experiment for Interior Structures), which measures "Mars' tectonic activity to learn more about its structure, for example the size of its core and the thickness of its mantle."[418] InSight landed on Mars in 2018 for its planned two-year mission, and in April 2019, the SEIS seismometer detected and recorded the first "Marsquake," allowing scientists to study the slight tremors detected on the Martian surface.[419]



Deployment of the SEIS Protection Dome on Mars.
NASA / JPL-CALTECH

Recent events have triggered changes in France's overall space policy. In September 2018, France publicly charged Russia with interfering with the operation of one of its satellites in GEO. The *Athena-Fidus*, a jointly operated French-Italian military satellite, provides broadband military communications. France alleged that the Russian satellite, known as *Luch* or *Olymp-K*, maneuvered close enough to *Athena-Fidus* in 2017 to intercept military communications.[420]

Following this public denunciation of Russian space activities, France issued a new Space Defense Strategy in 2019. Among other things, the French strategy calls for the creation of a Space Command under the Air Force and renaming the Air Force to the Air and Space Force. The strategy notes that "renewed analysis of the space environment and its threats, risks and opportunities, as well as the recognition of the strategic nature of the space assets for France force our country to revisit its model in order to remain a leading space power." The Space Defense Strategy further declares that France will establish a "space defense capacity" in order to "enable the armed forces to

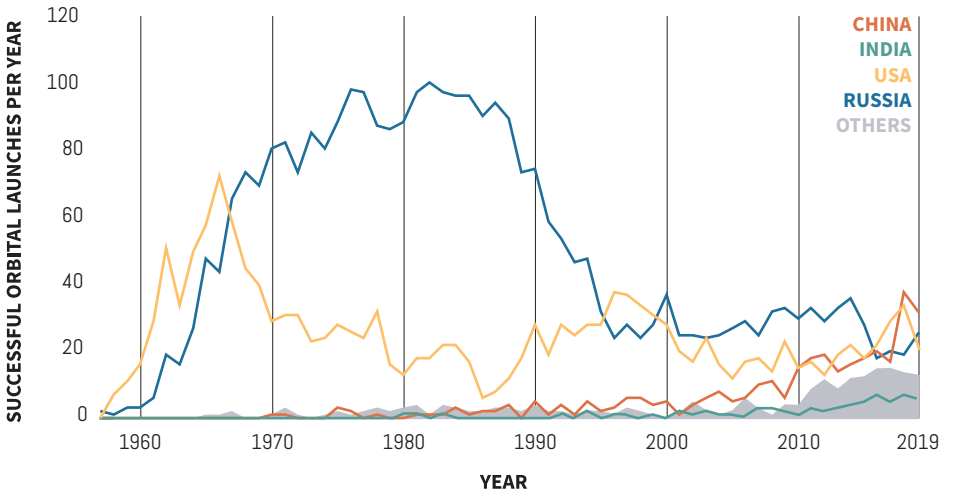


Figure 14: Space Orbital Launches from Other Nations (1957 - 2019). This figure includes orbital launches from nations such as New Zealand and Japan, as well as the European Space Agency.

SPACETRACK.ORG / CSIS AEROSPACE SECURITY[421]

impose a peaceful use of space, deter unfriendly or hostile acts against our space assets, and be able, as the case may be, to defend our space-based interests."[422] France has also committed to increasing its military space budget by 700 million euros between 2019 and 2025 to support the creation of Space Command and pursue "active defense" satellite technologies.[423] The defense of space assets appears to be in response to the interference France felt was caused by *Luch*.

In a speech announcing the new strategy, French Minister of the Armed Forces Florecne Parly spoke at length about the changes. In some of the most direct and specific language by a government official from any nation on space defense, the defense minister said, "I want to be precise: active defence is not an offensive strategy, what it is about is self-defence." She went on to add that, "If our satellites are threatened, we will consider dazzling those of our opponents. We reserve the time and means of the response: this may involve the use of high-power lasers deployed from our satellites or from our patrol nano-satellites."[424] Through these remarks Parly sheds further light on France's plans to develop and deploy "bodyguard" or "patrol" satellites to protect its space assets, as well as its plans to mount lasers on satellites in order to dazzle or blind satellites that may be threatening French assets.

A laser mounted on satellites is theoretically possible but faces some technological hurdles. Laura Grego from the Union of Concerned Scientists explained that "dazzling from accompanying satellites (probably not 'nano' satellites unless that definition is very generous) or onboard might stop other slow moving proximity operations satellites from observing their satellite [targets] or to make it hard for them to use lidar for getting really close." Dr. Grego went on to assert that it would be hard to use lasers on cross-orbit attacks or direct-ascent ASAT weapons.[425]

France's public posture toward protecting its space capabilities is shifting. The country's leaders are indicating a move toward active defense in space, which has contributed to a broader public debate on the proper use and development of counterspace weapons. While countries like China and Russia have been extensively developing offensive counterspace weapons, such as jamming and spoofing capabilities, France seems to be considering a different strategy: defensive capabilities on orbit. However, the country's policies appear to be in flux, and there is little public indication of how quickly France plans to pursue this new direction.

ISRAEL

In July 2019, the United States and Israel jointly tested the Arrow-3 missile interceptor. While not publicly listed as a direct-ascent ASAT weapon, "the Arrow-3 interceptor successfully demonstrated an engagement capability against the exo-atmospheric target during the test."[426] Speculation of the Arrow-3 system being used as an ASAT weapon began in 2009 when leading space military experts pointed out that "Israel's planned Arrow-3 high-altitude ballistic missile defense system could relatively easily be adapted to destroy Iranian spy satellites if and when Tehran manages to deploy high-resolution orbiting vehicles."[427]

The Israeli company Regulus claims to have spoofed a Tesla Model 3 using the Navigate on Autopilot (NOA) system.[428] The purpose of the NOA system is to follow a predetermined route maintained by using GPS and Google Maps technology. The spoofing targeted the relationship between the Tesla Model 3's NOA system and the GPS it relied on to maintain autopilot. The test itself took place on an interstate and made the car believe it was further along on the route, causing it to make an incorrect turn into a rest stop instead of the planned exit further down the road.[429] In response to these claims, Tesla stated that the test was only a promotional stunt and that they have no safety concerns with the Tesla-3's NOA.[430]

Israel has also begun development of a ground-based and plane-mounted high-energy laser defense system designed to target threats in the air. Currently it has no stated counterspace implications, but the technology could be adapted to perform some counterspace operations. With a power level of 50-100kW, this airborne laser could be capable of dazzling or even blinding satellites in LEO.[433]

Israeli Missile Interceptor, Arrow-3, was tested July 2019 out of the Pacific Spaceport in Alaska.[431] Designed to intercept medium-range ballistic missiles, the Arrow-3 system has been speculated to also be capable of performing direct-ascent anti-satellite operations.[432]

MISSILE DEFENSE AGENCY

JAPAN

In the past year, Japan has made progress toward setting up a new Space Domain Mission Unit, a military organization meant to protect Japanese space assets as more countries are moving to further weaponize space through the testing and development of kinetic and non-kinetic weapons.[434] Citing Japan's need "to protect itself from potential threats as rivals develop missiles and other technology," Prime Minister Shinzo Abe said this new organization will work closely with its American counterpart, the United States Space Force. The Space Domain Mission Unit will also cooperate with the newly re-established U.S. Space Command and Japan's own civil space agency, the Japan Aerospace Exploration Agency (JAXA).[435] With a small core established in 2020, the Space Domain Mission Unit plans to be fully operational in 2022 to "bolster capability and system[s] in order to secure space superiority."[436] After its establishment, the Space Domain Mission Unit will be responsible for operating the ground stations necessary to conduct these defense operations.[437]

Japan is also reportedly considering the development of active defenses to protect its space systems. Using robotic arm technology developed by JAXA, the Japanese government is debating options to develop a co-orbital satellite defense system to deter attacks on Japanese satellites. This system, which would intercept an attacking satellite in order to defend another Japanese space asset, could be launched as early as the mid-2020s.[438] The government is also reportedly considering options to disable hostile satellites through electronic and cyber means.[439]

In April of 2019, Japan deployed a *Hayabusa-2* probe system to an asteroid, Ryugu, which contained a small carry-on impactor (SCI). The SCI is an explosive projectile able to be launched at the asteroid to form an artificial crater. This explosive, which created rubble for Hayabusa-2 to collect and bring back to Earth as samples, could be placed on a satellite and be used as a co-orbital anti-satellite weapon.[440]

THE JAPANESE GOVERNMENT IS DEBATING OPTIONS TO DEVELOP A CO-ORBITAL SATELLITE DEFENSE SYSTEM.

Spoofing in the Mediterranean Sea

CIVIL AND COMMERCIAL MARINE GPS USERS reported consistent loss of GPS signal in the Mediterranean Sea and surrounding areas throughout 2019. These outages ranged from the coast of Libya to Greece and Egypt's Suez Canal. The U.S. Maritime Administration issued alerts that specifically mention the possibility of GPS interference in the Eastern and Central Mediterranean regions.[441] The increased instances of GPS jamming have led captains to suppress their AIS data and switch to receive only. This has led to a decrease in situational awareness on the sea.[442]

U.S. COAST GUARD NAVIGATION CENTER / EMILY TIEMEYER

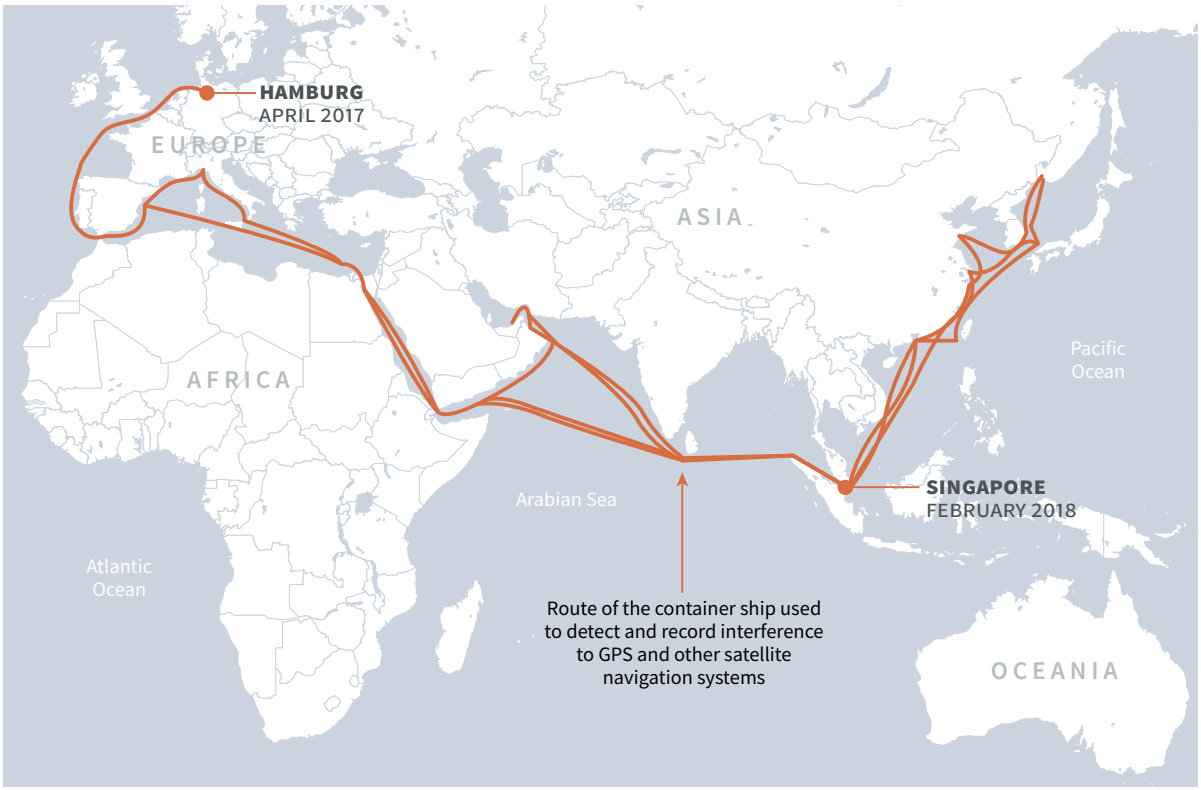


Figure 15: The Journey of the Basle Express. The Basle Express was a cargo ship outfitted with GPS receivers designed to track and collect GPS interference. The ship travelled from Germany to Singapore tracking and detailing many instances of GPS interference.

GERMAN AEROSPACE CENTER

UNITED KINGDOM

The United Kingdom has begun restructuring its military space organization, although it does not plan to create a separate military service for space. The current restructuring effort should result in a two-star major general becoming the director of Space within the Ministry of Defence, supported by policy and capabilities teams.[443] This comes after the U.K. government declared space as part of its critical national infrastructure in 2015 and more recently as a warfighting domain.[444] While the UK has not explicitly endorsed the development of space defense systems and counterspace weapons, the requisite technology is within its reach. For example, the United Kingdom is developing its own high-energy laser for anti-drone and missile defense. These lasers, while not directly cited as counterspace weapons, have the potential to be further developed into counterspace capabilities.[445]

NON-STATE ACTORS

In 2019, reports emerged of position, navigation, and timing (PNT) jamming in northeastern China, disrupting civilian aircraft flying over the area. Authorities were able to trace the jamming origin to a farm in Heilongjiang province near the city of Harbin. Frustrated by a local gang's hijinks of using drones to supposedly infect local farmers' pigs with African swine fever—a disease deadly to pigs, but harmless to humans—the farmer used PNT signal jamming to protect his herd. The gangs were infecting local pigs to force farmers to lower the prices and then would resell the pork to the public as "healthy" for the full price.[446]

In 2018, at Hong Kong's 10-year celebration of the Wine and Dine Festival, a drone light show over Victoria Harbor was disrupted by GPS jamming, which caused 46 drones to fall from the sky, resulting in $127,500 in damages.[447] In response to questions about the incident, the board's executive director, Anthony Lau Chun-hon, said that "the [jamming] signals were so strong that many of them just dropped from the air."[448]

In April of 2017, a commercial container ship, the *Basle Express*, left Hamburg, Germany on a research mission equipped with receivers designed to pick up on interference. The *Basle Express* mission was designed to sense levels of jamming and spoofing in different areas of the world.[449] While travelling around Europe, the Middle East, Africa, and Asia, the ship's crew detected strong interference "at some of the world's largest seaports, including Jeddah in Saudi Arabia, Singapore, Hong Kong, and Shanghai, and less often, on the open sea."[450] With many commercial vessels poorly suited to operating in a world where GPS is not guaranteed, some experts are recommending that new anti-jamming systems will need to be created to ensure that commercial shipping can continue unthreatened in an increasingly technology-dependent world.[451]

SUMMARY

In the last year, more states are considering the development of offensive and defensive counterspace capabilities to protect space systems from attacks. Nations are moving to reorganize their national security space enterprise, as the United States did in 2019, to better address the growing uncertainty and threats in the space domain. Jamming and spoofing technologies are also being used around the world by non-state actors in both conflict zones and thriving seaports, to gain military and economic advantage. Collectively, these developments are making the space environment more dynamic and uncertain—a trend that is likely to continue in the coming years.

WHAT TO WATCH

THIS YEAR'S EDITION OF THE CSIS SPACE THREAT ASSESSMENT finds that threats to space systems are growing as more countries and non-state actors acquire counterspace capabilities and, in some cases, employ them in more ways. While this report primarily details the developments in counterspace weapons that have occured in the last year, some of these developments have been ongoing for several years. This section highlights the types of threats and counterspace activities where more developments are expected to occur in the coming months and years.

Electronic counterspace weapons continue to proliferate at a rapid pace in both how they are used and who is using them. Satellite jamming and spoofing devices are becoming part of the every-day arsenal for countries that want to operate in the gray zone—i.e., below the threshold of overt conflict. The jamming and spoofing of satellites has become somewhat common, and without strong repercussions these adverse activities could gradually become normalized. The fact that Russian President Vladimir Putin appears to travel with GPS jamming devices in his motorcade and that China appears to be spoofing GPS signals to conceal illicit activities in its own ports demonstrate how important and integrated these capabilities have become at all levels. One should expect that the rate of satellite jamming and spoofing incidents will only increase as these capabilities continue to proliferate and become more sophisticated in the coming years.

One of the most significant counterspace developments in the past year was the Indian test of a direct-ascent ASAT weapon. This incident proved that a kinetic test done in a way that minimizes orbital debris may not generate the same degree of diplomatic backlash as the Chinese ASAT test in 2007. Moreover, the Indian test and how it was received could incentivize other nations, such as Pakistan, to develop and demonstrate ASAT capabilities of their own.

Russia also continued to step up its co-orbital activities in the past year. The Russian *Luch* satellite continued its close inspection of satellites in geostationary orbit, despite international denunciation of its activities. Russia also placed a widely-reported inspector around a classified U.S. Government satellite in low Earth orbit. Both the Indian ASAT test and Russia's co-orbital activities may provide further incentive for nations to develop and deploy defensive counterspace capabilities of their own, as France announced it intends to do. Nations may also seek to draw distinctions between offensive and defensive counterspace weapons in order to justify the latter while delegitimizing the former.

As nations reevaluate the threats to their space systems, some have moved to reorganize existing space organizations or create new military organizations to better focus on space as a warfighting domain. France is creating a Space Command within its military and renaming its Air Force the Air and Space Force, while the United Kingdom may not be far behind in reorganizing its space forces. In the coming years, more nations may continue to reorganize and elevate space forces within their militaries both to focus attention internally and to signal externally.

A final area to watch in the coming year is how the United States continues to adapt to face threats in the space domain. The U.S. military is in the midst of what is arguably the most significant reorganization since the Goldwater-Nichols Act of 1986. With the re-establishment of United States Space Command as a geographic combatant command for space and the new establishment of the Space Force as an independent military service for space, many things are in flux within the military space community. While there is great opportunity in this reorganization process, there are many risks as well. A chief concern is that an excessive focus on building bureaucracy (and attempts to limit bureaucracy) could distract senior leaders' attention from the evolving threats to space systems and the U.S. military's efforts to counter these threats. Key developments to watch within the United States are updates to space doctrine, strategy, and policy and investments in new space capabilities and missions. Developments in these areas would be a clear indication that the reorganization efforts put in place in 2019 are part of a fundamental shift in the U.S. military's overall approach to making space more defendable.

ABOUT THE AUTHORS

TODD HARRISON is the director of the Aerospace Security Project and the director of Defense Budget Analysis 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 space security, air power, and defense funding issues. 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 a small startup (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 an associate fellow and associate director of the CSIS Aerospace Security Project. 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.

THOMAS G. ROBERTS is an adjunct fellow with the CSIS Aerospace Security Project, a graduate researcher at the Massachusetts Institute of Technology (MIT) Space Systems Laboratory, and an SM candidate in MIT's Department of Aeronautics and Astronautics and Technology and Policy Program. His research interests include orbital mechanics, astrodynamics, and international space policy. Previously, Mr. Roberts has written on space-based missile defense, threats against space-based assets, and human spaceflight programs. His work has appeared in *The Atlantic, War on the Rocks, The Bulletin of the Atomic Scientists,* and other publications. Mr. Roberts holds a BA in astrophysical sciences with honors and an undergraduate certificate in Russian studies from Princeton University. In 2015, he was named a Harry S. Truman Scholar.

TYLER WAY is a research intern for the CSIS Aerospace Security Project. His research focuses on the applications of space within national security as well as the role of space in socioeconomic development. He is currently a graduate student at George Washington University's Elliott School, pursuing an MA in International Science and Technology Policy in the Space Policy Institute. Tyler holds a BA in International Studies from Bowling Green State University in Bowling Green, Ohio.

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

APPENDIX I

LIST OF ACRONYMS USED

A2/AD	Anti-Access/Area Denial
AEHF	Advanced Extremely High Frequency
AIS	Automatic Identification System
APT 28	Russian Hacker Group
ASAT	Anti-Satellite
BBC	British Broadcasting Corporation
C4ADS	Center for Advanced Defense Studies
C4ISR	Command, Control, Communications, Computers (C4), Intelligence, Surveillance, and Reconnaissance (ISR)
CASC	China Aerospace Science and Technology Corporation
CHEOS	China High-resolution Earth Observation System
CNES	National Centre for Space Studies (France)
CNSA	China National Space Administration
CSS	Chinese Space Station
DCA	Defence Cyber Agency (India)
DDOS	Distributed Denial of Service
DIA	Defense Intelligence Agency
DoD	U.S. Department of Defense
DPRK	Democratic People's Republic of Korea
DSA	Defence Space Agency (India)
DSN	Deep Space Network
DSRO	Defence Space Research Organization (India)
EMP	Electromagnetic Pulse
ESA	European Space Agency
EW	Electronic Warfare
FSO	Federal Protective Service
GBS	Global Broadcast Service
GEO	Geosynchronous Orbit
GNSS	Global Navigation Satellite System (Russia)
GPS	Global Positioning System
GSLV	Geosynchronous Satellite Launch Vehicle
HPM	High Powered Microwave
ICBM	Intercontinental Ballistic Missile
IRGC	Islamic Revolutionary Guard Corps
IS	Istrebitel Sputnikov (Russia)
ISA	Israel Space Agency
ISRO	Indian Space Research Organization
ISS	International Space Station

JAXA	Japan Aerospace Exploration Agency
JCPOA	Joint Comprehensive Plan of Action
JPL	Jet Propulsion Laboratory
JSOC	Joint Special Operations Command
KCNA	Korean Central News Agency (North Korea)
LEO	Low Earth Orbit
MEO	Medium Earth Orbit
MMW	Millimeter Wave
NADA	National Aerospace Development Administration (North Korea)
NASA	National Aeronautics and Space Administration
NIIPKh	Scientific Research Institute of Applied Chemistry (Russia)
NOA	Navigate on Autopilot
NOAA	National Oceanographic and Atmospheric Administration
NOTAM	Notice to Airmen
NRO	U.S. National Reconnaissance Office
PDV-Mk II	Prithvi Delivery Vehicle Mark-II (India)
PLA	People's Liberation Army (China)
PNT	Positioning, Navigation, and Timing
PSLV	Polar Satellite Launch Vehicle
RF	Radio Frequency
RGB	Reconnaissance General Bureau (North Korea)
RPO	Rendezvous and Proximity Operations
SASTIND	State Administration for Science, Technology, and Industry for National Defense
SATCOM	Satellite Communications
SCI	Small Carry-On Impactor
SEIS	Seismic Experiment for Interior Structures
SLV	Space Launch Vehicle
SSF	Strategic Support Force (China)
SSLV	Small Satellite Launch Vehicle (India)
SSO	Sun-Synchronous Orbit
TEL	Transporter erector-launcher
UH	Ultra High Frequency
UK	United Kingdom
VOA	Voice of America
WGS	Widespread Global SATCOM (Satellite Communications)

ENDNOTES

TYPES OF COUNTERSPACE WEAPONS

1 Office of the President of the United States, *National Security Strategy* (Washington, DC: December 2017), 31, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

2 Office of Technology Assessment, Anti-Satellite Weapons, Countermeasures, and Arms Control (Washington, DC: Government Printing Office, September 1985), 7, https://apps.dtic.mil/dtic/tr/fulltext/u2/a335693.pdf.

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

4 David Wright, Laura Grego, and Lisbeth Gronlund, *The Physics of Space Security: A Reference Manual* (Cambridge, MA: American Academy of Arts and Sciences, 2005), 131-132, https://www.amacad.org/sites/default/files/publication/downloads/Physics_of_Space_Security.pdf.

5 Steven James Lambakis, *On the Edge of Earth: The Future of American Space Power* (Lexington, KY: University Press of Kentucky, 2001), 123.

6 Garino and Gibson, "SpaceSystem Threats," 274-275.

7 Sydney J. Freedberg, Jr., "US Jammed Own Satellites 261Times; What If Enemy Did?," Breaking Defense, December 2, 2015, http://break ingdefense.com/2015/12/us-jammed-own-satellites-261-times-in-2015-what-if-an-enemy-tried/.

8 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-ra pid-antenna-motion/.

9 Allie Sanchez, "Cyber Attacks Available for Hire," Insurance Business America, April 3, 2017, https://www.insurancebusinessmag.com/us/ news/cyber/cyber-attacks-available-for-hire-64287.aspx.

CHINA

10 "Space Environment: Total Launches by Country," Aerospace Security Program, last updated January 2, 2020, https://aerospace.csis.org/data/space-environment-total-launches-by-country/.

11 Dave Makichuk, "China's Bold Space Program Flourishing: Article," *Asia Times*, November 5, 2019, https://www.asiatimes.com/2019/11/article/chinas-bold-space-program-flourishing.

12 "Space Environment: Total Launches by Country," Aerospace Security Program.

13 "China reveals space plan for 2020," Xinhua News Agency, January 17, 2020, http://www.xinhuanet.com/english/2020-01/17/c_138713906.htm.

14 Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2019* (Washington, DC: U.S. Department of Defense, May 2019), 49, https://media.defense.gov/2018/Aug/16/2001955282/-1/-1/1/2018-CHINA-MILITARY-POWER-REPORT.PDF.

15 Andrew Jones, "China's First Mars Spacecraft Undergoing Integration for 2020 Launch," SpaceNews, May 29, 2019, https://spacenews.com/chinas-first-mars-spacecraft-undergoing-integration-for-2020-launch; Andrew Jones, "Rocket Nears Spaceport for Chinese Space Station Test Launch," SpaceNews, January 31, 2020, https://spacenews.com/rocket-nears-spaceport-for-chinese-space-station-test-launch/.

16 Xinhua News Agency "China's Long March-5B carrier rocket arrives at launch site," China.org, February 6, 2020, http://www.china.org.cn/china/2020-02/06/content_75677139.htm.

17 Jones, "Rocket Nears Spaceport for Chinese Space Station Test Launch."

18 Namrata Goswami, "China's Future Space Ambitions: What's Ahead?," *Diplomat*, November 4, 2019, https://thediplomat.com/2019/11/chinas-future-space-ambitions-whats-ahead/.

19 "Space Environment: Total Payloads Launched by Country," accessed February 12, 2020.

20 "What's driving China's race to build a space station?," ChinaPower, CSIS, December 7, 2016, https://chinapower.csis.org/chinese-space-station/.

21 Andrew Jones, "Chinese Space Station Core Module Passes Review but Faces Delays," SpaceNews, September 12, 2019, https://spacenews.com/chinese-space-station-core-module-passes-review-but-faces-delays/.

22 Ibid.; Yamei Liwei Yang, "China readying for space station era," *Xinhua News Agency*, July 8, 2018, http://www.xinhuanet.com/english/2018-07/08/c_137310103.htm.

23 Ludovic Ehret, "China Unveils New 'Heavenly Palace' Space Station as ISS Days Numbered," Phys.org, November 6, 2018, https://phys.org/news/2018-11-china-unveils-heavenly-palace-space.html.

24 Office of Outer Space Affairs, "The United Nations/China Cooperation on the Utilization of the China Space Station," United Nations, June 19, 2020, https://www.unoosa.org/oosa/en/ourwork/psa/hsti/chinaspacestation/1st_cycle_2018.html.

25 U.S.-China Economic and Security Review Commission, "2019 Report to Congress of the U.S.-China Economic and Security Review Commission" (Washington, DC: U.S. Government Publishing Office, 2019), 368, https://www.uscc.gov/sites/default/files/2019-11/2019%20Annual%20Report%20to%20Congress.pdf; Andrew Jones, "China, Russia to Cooperate on Lunar Orbiter, Landing Missions," *Space News*, September 19, 2019, https://spacenews.com/china-russia-to-cooperate-on-lunar-orbiter-landing-missions/.

26 Thomas G. Roberts, *Spaceports of the World*, Aerospace Security Project, CSIS, accessed February 12, 2020, https://aerospace.csis.org/data/spaceports-of-the-world/.

27 Andrew Jones, "China Creates Commercial Space Alliance, Expands Launch Complex," SpaceNews, December 20, 2019, https://spacenews.com/china-creates-commercial-space-alliance-expands-launch-complex/.

28 Roberts, “Spaceports of the World.”

29 Meng Jing, “China Rolls out Rules on Commercial Space Rocket Development,” *South China Morning Post*, June 12, 2019, https://www.scmp.com/tech/science-research/article/3014157/china-rolls-out-rules-guide-development-spacex-style.

30 Jing, “China Rolls out Rules on Commercial Space Rocket Development”; Andrew Jones, “Chinese Commercial Launch Sector Regulations Released, New Launch Vehicle Plans Unveiled,” SpaceNews, July 2, 2019, https://spacenews.com/chinese-commercial-launch-sector-regulations-released-new-launch-vehicle-plans-unveiled.

31 Marco Aliberti, *When China Goes to the Moon...* (Switzerland: Springer International Publishing, 2015), 7-19, https://www.springer.com/cda/content/document/cda_downloaddocument/9783319194721-c1.pdf?SGWID=0-0-45-1513274-p177396349.

32 Dennis J. Blasko, “Steady as She Goes: China’s New Defense White Paper,” War on the Rocks, August 9, 2019, https://warontherocks.com/2019/08/steady-as-she-goes-chinas-new-defense-white-paper.

33 Li Jiayao, ed., “China’s National Defense in the New Era,” Ministry of National Defense of the People’s Republic of China, Xinhua News Agency, July 24, 2019, http://eng.mod.gov.cn/news/2019-07/24/content_4846443.htm.

34 Ibid.

35 The State Council Information Office of the People’s Republic of China, *China’s Military Strategy* (Beijing, China: People’s Republic of China, May 2015), http://eng.mod.gov.cn/Press/2015-05/26/content_4586805.htm.

36 Kevin Pollpeter, Michael Chase, and Eric Heginbotham, *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations* (Santa Monica, CA: RAND Corporation, 2017), 3-4, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2058/RAND_RR2058.pdf.

37 Ibid., 7.

38 Office of the Secretary of Defense, “Annual Report to Congress: Military Power of the People’s Republic of China 2019,” 13.

39 United States Congress, U.S. - China Economic and Security Review Commission, *Hearing on China’s Military Reforms and Modernization: Implications for the United States,* 115th Cong., 2nd sess., February 15, 2018, 40, https://www.uscc.gov/sites/default/files/transcripts/Hearwing%20Transcript%20-%20February%2015%2C%202018.pdf.

40 National Air and Space Intelligence Center, *Competing in Space* (Wright Patterson Air Force Base: Ohio, December 2018), 21, https://media.defense.gov/2019/Jan/16/2002080386/-1/-1/1/190115-F-NV711-0002.PDF.

41 U.S.-China Economic and Security Review Commission, *2019 Report to Congress*, 375.

42 Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People’s Republic of China 2019*, 49.

43 U.S.-China Economic and Security Review Commission, “2015 Report to Congress of the U.S.-China Economic and Security Review Commission” (Washington, DC: U.S. Government Publishing Office, 2015), 294,https://www.uscc.gov/sites/default/files/annual_reports/2015%20Annual%20Report%20to%20Congress.PDF.

44 Independent analysis by Kaitlyn Johnson; data from “Space-Track,” Space-Track, www.space-track.org.

45 Brian Weeden and Victoria Samson, eds., *Global Counterspace Capabilities: An Open Source Assessment* (Broomfield, Colorado: Secure World Foundation, 2018), 1–11, https://swfound.org/media/206118/swf_global_counterspace_april2018.pdf.

46 U.S. Defense Intelligence Agency, *China Military Power: Modernizing a Force to Fight and Win*, (Washington, DC: 2018), 43, http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/China_Military_Power_FINAL_ 5MB_20190103.pdf.

47 U.S.-China Economic and Security Review Commission, *2015 Report to Congress*, 294.

48 “SC-19 Anti-Ballistic Missile Interceptor,” *GlobalSecurity.org*, last updated July 25, 2016, https://www.globalsecurity.org/space/world/china/sc-19-abm.htm.

49 Li Bin, “What China’s Missile Intercept Test Means,” Carnegie Endowment for International Peace, February 4, 2013, https://carnegieendowsment.org/2013/02/04/what-china-s-missile-intercept-test-means-pub-50833.

50 Brian Weeden, “Anti-Satellite Tests in Space - The Case of China,” Secure World Foundation, updated May 18, 2015, https://swfound.org/media/115643/china_asat_fact_sheet_may2015.pdf.

51 “China Tests Missile Intercept System,” Nuclear Threat Initiative, January 28, 2013, https://www.nti.org/gsn/article/china-tests-missile-intercept-system; Bin, “What China’s Missile Intercept Test Means.”

52 Mike Gruss, “Pentagon Says 2013 Chinese Launch May Have Tested Antisatellite Technology,” SpaceNews, May 14, 2015, https://spacenews.com/pentagon-says-2013-chinese-launch-may-have-tested-antisatellite-technology.

53 Weeden, “Anti-Satellite Tests in Space - The Case of China.”

54 Gruss, “Pentagon Says 2013 Chinese Launch May Have Tested Antisatellite Technology.”

55 Mike Gruss, “U.S. State Department: China Tested Anti-Satellite Weapon,” SpaceNews, January 30, 2015, https://spacenews.com/41413us-state-department-china-tested-anti-satellite-weapon.

56 Bill Gertz, “China Tests Anti-Satellite Missile,” Washington Free Beacon, November 9, 2015, https://freebeacon.com/national-security/china-tests-anti-satellite-missile/.

57 Ibid.

58 Bill Gertz, “China Carries Out Flight Test of Anti-Satellite Missile,” Washington Free Beacon, August 2, 2017, https://freebeacon.com/national-security/china-carries-flight-test-anti-satellite-missile.

59 Ankit Panda, “Revealed: The Details of China’s Latest Hit-To-Kill Interceptor Test,” *Diplomat*, February 21, 2018, https://thediplomat.com/2018/02/revealed-the-details-of-chinas-latest-hit-to-kill-interceptor-test.

60 U.S.-China Economic and Security Review Commission, *2019 Report to Congress*, 382.

61 Ibid.

62 Brian Weeden, "China's BX-1 microsatellite: a litmus test for space weaponization," The Space Review, October 20, 2008, http://www.thespacereview.com/article/1235/1.

63 Weeden and Samson, eds., *Global Counterspace Capabilities*, 1-2.

64 U.S.-China Economic and Security Review Commission, *2015 Report to Congress*, 295.

65 Brian Weeden, "Dancing in the dark: The orbital rendezvous of SJ-12 and SJ-06F," The Space Review, August 10, 2010, http://www.thespacereview.com/article/1689/1.

66 Pollpeter, et al., *The Creation of the PLA Strategic Support Force*, 10.

67 "China Successfully Launches Three Satellites," *Economic Times*, July 20, 2013, https://economictimes.indiatimes.com/china-successfully-launches-three-satellites/articleshow/21187532.cms.

68 U.S.-China Economic and Security Review Commission, *2015 Report to Congress*, 295; Weeden and Samson, eds., *Global Counterspace Capabilities*, 1-2.

69 Ibid.; "China's new Orbital Debris Clean-Up Satellite raises Space Militarization Concerns," *Spaceflight 101*, June 29, 2016, http://spaceflight101.com/long-march-7-maiden-launch/aolong-1-asat-concerns/.

70 Stephen Chen, "How China's Scavenger Satellites Are Being Used to Develop AI Weapons," *South China Morning Post*, April 22, 2019, https://www.scmp.com/news/china/science/article/3007186/how-chinas-scavenger-satellites-are-being-used-develop-ai.

71 "China announces success in technology to refuel satellites in orbit," *Xinhua News Agency*, June 30, 2016, http://www.xinhuanet.com/english/2016-06/30/c_135479061.htm.

72 Internal CSIS analysis by Thomas G. Roberts; data from "Space-Track," www.space-track.org.

73 Stephen Chen, "How China's Scavenger Satellites Are Being Used to Develop AI Weapons."

74 SJ-17 is estimated to have a mass around 4,000kg. Gunter Dirk Krebs, "SJ 17," Gunter's Space Page, last updated July 21, 2019, https://space.skyrocket.de/doc_sdat/sj-17.htm.

75 International Institute for Strategic Studies, *The Military Balance 2017* (London: Routledge, 2017), 19-26, https://www.iiss.org/publications/the-military-balance/the-military-balance-2017.

76 Aaron Mehta, "Chinese Threats Necessitate New Space Structures, Shanahan Warns," *Defense News*, April 9, 2019, https://www.defensenews.com/space/2019/04/09/chinese-threats-necessitate-new-space-structures-shanahan-warns.

77 Daniel R. Coats, "Worldwide Threat Assessment of the US Intelligence Community," Office of the Director of National Intelligence, February 13, 2018, 13, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

78 Vago Muradian, "China Tried to Blind U.S. Sats with Laser," *Defense News*, September 25, 2006, https://www.ar15.com/forums/general/China_Tried_To_Blind_U_S__Sats_With_Laser/5-501978/.

79 Andrea Shalal-Esa, "China Jamming Test Sparks U.S. Satellite Concerns," Reuters, October 5, 2006, as quoted in Yousaf Butt, "Effects of Chinese Laser Ranging on Imaging Satellites," *Science & Global Security*, 17:1, 2009, 20-35.

80 Edwin Cartlidge, "Physicists are planning to build lasers so powerful they could rip apart empty space," *Science*, January 24, 2018, http://www.sciencemag.org/news/2018/01/physicists-are-planning-build-lasers-so-powerful-they-could-rip-apart-empty-space.

81 Timothy Grayson, "Prepared Statement of Dr. Timothy Grayson," Testimony before the U.S.-China Economic and Security Review Commission, Hearing on China's Advanced Weapons, February 23, 2017, 70, https://www.uscc.gov/sites/default/files/transcripts/China%27s%20Advanced%20Weapons.pdf.

82 John J. Raymond, (remarks, Mitchell Institute for Aerospace Studies, Washington, DC), reported by Mandy Mayfield, "JUST IN: Space Commander Warns Chinese Lasers Could Blind U.S. Satellites," *National Defense Magazine*, September 27, 2019, https://www.nationaldefensemagazine.org/articles/2019/9/27/space-commander-warns-chinese-lasers-could-blind-us-satellites.

83 U.S. Defense Intelligence Agency, *Challenges to Security in Space*, (Washington, D.C.: U.S. Defense Intelligence Agency, February 2019), 20, http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.

84 David D. Chen, "Opening Statement of Mr. David Chen," Testimony before the U.S.-China Economic and Security Review Commission, February 23, 2017, 75, https://www.uscc.gov/sites/default/files/transcripts/China%27s%20Advanced%20Weapons.pdf.

85 Mark Stokes, "Prepared Statement of Mark A. Stokes," Testimony before the U.S.-China Economic and Security Review Commission, April 25, 2019, 4, https://www.uscc.gov/sites/default/files/Mark%20Stokes%20USCC%2025%20April.pdf.

86 Dylan Malyasov, "China Discloses New Directed-Energy Weapon Development," Defence Blog, April 4, 2019,

87 Liu Xuanzun, "Arms Firm Makes Artificial Diamonds That Could Be Used in Laser Weapons," *Global Times*, December 4, 2019, https://www.globaltimes.cn/content/1172265.shtml.

88 Vinayak Bhat, "These Futuristic Chinese Space Denial Weapons Can Disable or Destroy Opposing Satellites," *The Print*, March 23, 2019, https://theprint.in/defence/these-futuristic-chinese-space-denial-weapons-can-disable-or-destroy-opposing-satellites/210212/.

89 Bill Gertz, "Satellite Photos Show Chinese Anti-Satellite Laser Base," Washington Free Beacon, March 31, 2019, https://freebeacon.com/national-security/satellite-photos-show-chinese-anti-satellite-laser-base/.

90 Liu Zhen, "Chinese Military Hints at Plans for Airborne Laser Attack Weapon," *South China Morning Post*, January 7, 2020, https://www.scmp.com/news/china/military/article/3045066/chinese-military-hints-plans-airborne-laser-attack-weapon.

91 Richard D. Fisher, Jr., "China's Progress with Directed Energy Weapons," Testimony before the U.S.-China Economic and Security Review Commission, February 23, 2017, 9, https://www.uscc.gov/sites/default/files/Fisher_Combined.pdf.

92 U.S.-China Economic and Security Review Commission, *2015 Report to Congress*, 298.

93 U.S. Defense Intelligence Agency, *Challenges to Security in Space*, 20.

94 Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2018* (Washington, DC: U.S. Department of Defense, May 2018), 21, https://media.defense.gov/2018/Aug/16/2001955282/-1/-1/1/2018-CHINA-MILITARY-POWER-REPORT.PDF.

95 U.S.-China Economic and Security Review Commission, *2015 Report to Congress*, 297-298.

96 U.S. Defense Intelligence Agency, *Challenges to Security in Space*, 20; Lin Jinshun et al., "Study on Countermeasure against Satellite Adaptive Null-Steering Technique," *Aerospace Electronic Warfare* 26, no. 3 (March 2010): 1-4, http://en.cnki.com.cn/Article_en/CJFDTotal-HTDZ201003000.htm; and H. Wang, "Analysis on Anti-jamming Measures of Mobile User Objective System," Radio Communications Technology 35, no. 2 (2009): 46-49.

97 Lin Jin-shun, et al., "Countermeasure Technology for MMW Satellite Links," *Aerospace Electronic Warfare*, October 2012, 20–22, http://en.cnki.com.cn/Article_en/CJFDTotal-HTDZ201205006.htm, as quoted in David D. Chen, "Opening Statement of Mr. David Chen," 82.

98 Bill Gertz, "Inside the Ring: China targets Global Hawk drone," *Washington Times*, December 11, 2013, https://www.washingtontimes.com/news/2013/dec/11/inside-the-ring-china-targets-global-hawk-drone/.

99 Liu Xuanzun, "China Capable of Defending against Deadly Drone Attacks: Experts," *Global Times*, January 5, 2020, https://www.globaltimes.cn/content/1175804.shtml.

100 Michael R. Gordon and Jeremy Page, "China Installed Military Jamming Equipment on Spratly Islands, U.S. Says," *Wall Street Journal*, April 9, 2018, https://www.wsj.com/articles/china-installed-military-jamming-equipment-on-spratly-islands-u-s-says-1523266320.

101 "Vietnam Demands That China Remove Military Jamming Equipment from Spratly Islands," *VnExpress* International, April 26, 2018, https://e.vnexpress.net/news/news/vietnam-demands-that-china-remove-military-jamming-equipment-from-spratly-islands-3741545.html.

102 U.S. Defense Intelligence Agency, *China Military Power: Modernizing a Force to Fight and Win*, 23 and 49.

103 Sebastien Roblin, "Why China's J-16D Electronic Warfare Plane Is a Really Big Deal," *National Interest*, November 20, 2019, https://nationalinterest.org/blog/buzz/why-chinas-j-16d-electronic-warfare-plane-really-big-deal-97677.

104 Dana Goward, "GPS Jamming and Spoofing Reported at Port of Shanghai," Maritime Executive, August 13, 2019, https://www.maritime-executive.com/editorials/gps-jamming-and-spoofing-at-port-of-shanghai; Mark Harris, "Ghost Ships, Crop Circles, and Soft Gold: A GPS Mystery in Shanghai," *MIT Technology Review*, November 20, 2019, https://www.technologyreview.com/s/614689/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai; 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.

105 "GPS Problem Report Status," U.S. Coast Guard Navigation Center, accessed February 13, 2020, https://navcen.uscg.gov/?Do=GPSReportStatus#definition.

106 Harris, "Ghost Ships, Crop Circles, and Soft Gold: A GPS Mystery in Shanghai."

107 Tyler Rogoway, "China's Mysterious Spoofed GPS 'Crop Circle' Has Something Interesting At Its Center," The Drive, November 19, 2019, https://www.thedrive.com/the-war-zone/31098/chinas-mysterious-spoofed-gps-data-crop-circle-has-something-interesting-at-its-center.

108 Harris, "Ghost Ships, Crop Circles, and Soft Gold: A GPS Mystery in Shanghai."

109 Bjorn Bergman, "Systematic GPS Manipulation Occuring at Chinese Oil Terminals and Government Installations," SkyTruth, December 16, 2019, https://skytruth.org/2019/12/systematic-gps-manipulation-occuring-at-chinese-oil-terminals-and-government-installations.

110 Ibid.

111 Harris, "Ghost Ships, Crop Circles, and Soft Gold: A GPS Mystery in Shanghai."

112 U.S. Defense Intelligence Agency, *Challenges to Security in Space*, 21.

113 Ibid., 20-21.

114 The State Council Information Office of the People's Republic of China, *China's Military Strategy* (Beijing, China: People's Republic of China, May 2015), http://eng.mod.gov.cn/Press/2015-05/26/content_4586805.htm.

115 U.S.-China Economic and Security Review Commission, *2015 Report to Congress*, 296.

116 U.S. Defense Intelligence Agency, *China Military Power*, 46.

117 U.S.-China Economic and Security Review Commission, *2015 Report to Congress*, 296.

118 Sui-Lee Wee, "China Denies It Is behind Hacking of U.S. Satellites," Reuters, October 31, 2011, https://www.reuters.com/article/us-china-us-hacking/china-denies-it-is-behind-hacking-of-u-s-satellites-idUSTRE79U1YI20111031.

119 U.S.-China Economic and Security Review Commission, *2015 Report to Congress*, 296.

120 NASA Office of the Inspector General, *Cybersecurity Management and Oversight at the Jet Propulsion Laboratory Washington, DC: 2019),* 8-9, https://oig.nasa.gov/docs/IG-19-022.pdf.

121 Ibid.

122 Mary Pat Flaherty, Jason Samenow and Lisa Rein, "Chinese hack U.S. weather systems, satellite network," *Washington Post*, November 12, 2014, https://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html.

123 Yatish Yadav, "Hackers from China Break into Secret Indian Government Video Chat," *New Indian Express*, November 19, 2017, http://www.newindianexpress.com/nation/2017/nov/19/hackers-from-china-break-into-secret-indian-government-video-chat-1705010.html.

124 Chris Bing, "Chinese Hacking Group Resurfaces, Targets U.S. Satellite Companies and Systems," *Cyberscoop*, June 19, 2018, https://www.cyberscoop.com/symantec-thrip-satellite-hacking-trojans/.

125 Joel Schectman and Christopher Bing, "UAE Used Cyber Super-weapon to Spy on IPhones of Foes," Reuters, January 30, 2019, https://www.reuters.com/article/us-usa-spying-karma-exclusive/exclusive-uae-used-cyber-super-weapon-to-spy-on-iphones-of-foes-idUSKCN-1PO1AN.

126 Sean O'Kane, "Chinese Hackers Charged with Stealing Data from NASA, IBM, and Others," The Verge, December 20, 2018, https://www.theverge.com/2018/12/20/18150275/chinese-hackers-stealing-data-nasa-ibm-charged.

127 Internal CSIS analysis by Thomas G. Roberts; data from "Space-Track," Space-Track, www.space-track.org.

RUSSIA

128 "Orbital Launches of 2019," Gunter's Space Page, February 11, 2020, https://space.skyrocket.de/doc_chr/lau2019.htm.

129 "О Развитии Государственной Корпорации По Космической Деятельности «Роскосмос»," Правительство России, Translated by Thomas G. Roberts, June 13, 2019, http://government.ru/news/36999/#.

130 Maxim V. Tarasenko, "Transformation of the Soviet Space Program after the Cold War," *Science & Global Securit*y 4, no. 3 (1994): 339-361, https://doi.org/10.1080/08929889408426406, 346).

131 Thomas G. Roberts, *Spaceports of the World* (Washington, DC: CSIS, March 2019), https://aerospace.csis.org/spaceports-of-the-world/; "UCS Satellite Database," Union of Concerned Scientists, accessed February 10, 2020, https://www.ucsusa.org/resources/satellite-database; Simon Seminari, "Op-Ed: Global Government Space Budgets Continues Multiyear Rebound," SpaceNews, November 24, 2019, https://spacenews.com/op-ed-global-government-space-budgets-continues-multiyear-rebound/; and Laurence Peter, "Russia Corruption: Putin's Pet Space Project Vostochny Tainted by Massive Theft," BBC News November 19, 2019, https://www.bbc.com/news/world-europe-50462431.

132 "Space Environment: Total Payloads Launched by Country," Aerospace Security Project, CSIS, accessed February 28, 2019, https://aerospace.csis.org/data/space-environment-total-launches-country/.

133 "Partners Sign ISS Agreements," NASA, October 23, 2010, https://www.nasa.gov/mission_pages/station/structure/elements/partners_agreement.html.

134 Thomas G. Roberts, "International Astronaut Database," Aerospace Security Project, CSIS, accessed February 10, 2020, https://aerospace.csis.org/data/international-astronaut-database/.

135 Anatoly Zak, "Russian space program in the 2010s: decadal review," Russian Space Web, February 11, 2019, http://www.russianspaceweb.com/russia_2010s.html#2019; Mike Wall, "Here's How Much NASA Is Paying Per Seat on SpaceX's Crew Dragon & Boeing's Starliner," Space.com, November 16, 2019, https://www.space.com/spacex-boeing-commercial-crew-seat-prices.html.

136 NASA Office of the Inspector General, '"NASA's Commercial Crew Program: Update on Development and Certification Effort," September 1, 2016, 27, https://oig.nasa.gov/docs/IG-16-028.pdf; and Christian Davenport, "SpaceX Completes Key Test of Its Dragon Capsule. Its First Human Spaceflight Might Come in Spring," *Washington Post*, January 19, 2020, https://www.washingtonpost.com/technology/2020/01/19/spacexemergencyabortttest/.

137 Andrew Jones, "China, Russia to Cooperate on Lunar Orbiter, Landing Missions," SpaceNews, September 20, 2019, https://spacenews.com/china-russia-to-cooperate-on-lunar-orbiter-landing-missions/.

138 Roberts, *Spaceports of the World*, 21.

139 Jeff Foust, "Space agencies endorse continued cooperation in lunar exploration," SpaceNews, October 21, 2019, https://spacenews.com/space-agencies-endorse-continued-cooperation-in-lunar-exploration/.

140 "'No End in Sight' to Fraud in Russia's Space Agency, Top Investigator Says," *Moscow Times*, May 17, 2019, https://www.themoscowtimes.com/2019/05/17/no-end-in-sight-russias-space-agency-top-investigator-says-a65618.

141 Victoria Loguinova-Yakoleva, "Russian space sector plagued by astronomical corruption," Space Daily, May 28, 2019, https://www.spacedaily.com/reports/Russian_space_sector_plagued_by_astronomical_corruption_999.html.

142 Madeline Roache, "Putin's Vostochny Project Meant to Reestablish Russia as a Space Superpower. Now It's Plagued by Corruption," *TIME*, November 19, 2019, https://time.com/5732370/putin-vostochny-space-center-theft/.

143 "'No End in Sight' to Fraud in Russia's Space Agency, Top Investigator Says," *Moscow Times*.

144 Eric Berger, "How Russia (yes, Russia) plans to land cosmonauts on the Moon by 2030," Ars Technica, May 28, 2019, https://arstechnica.com/science/2019/05/how-russia-yes-russia-plans-to-land-cosmonauts-on-the-moon-by-2030/.

145 Michael Kofman, "Russian defense spending is much larger, and more sustainable than it seems," Defense News, May 3, 2019, https://www.defensenews.com/opinion/commentary/2019/05/03/russian-defense-spending-is-much-larger-and-more-sustainable-than-it-seems/.

146 Note: Included in the Russian Federal Space Agency's inheritance from the Soviet Union was an active crewed mission—the Mir space station—with a Soviet cosmonaut still in orbit when the Russian Federation was founded; Elizabeth Howell, "Roscosmos: Russia's Space Agency," Space.com, January 29, 2018, https://www.space.com/22724-roscosmos.html; and Eric Betz, "The Last Soviet Citizen," *Discover Magazine*, December 19, 2016, https://www.discovermagazine.com/the-sciences/the-last-soviet-citizen.

147 "Roscosmos General Information," Roscosmos, n.d., accessed February 5, 2020, http://en.roscosmos.ru/119/; and "International Cooperation," NASA, February 28, 2019, https://www.nasa.gov/mission_pages/station/cooperation/index.html.

148 "Space Environment: Total Payloads Launched by Country," accessed February 12, 2020.

149 Matthew Bodner, "As Trump Pushes for Separate Space Force, Russia Moves 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/.

150 Matthew Bodner, "Russia Merges AF with Missile Defense, Space Commands," *Defense News*, August 8, 2015, https://www.defensenews.com/2015/08/08/russia-merges-af-with-missile-defense-space-commands/; and Ministry of Defence of the Russian Federation, "Aerospace Defence Forces," Russian Federation, n.d., accessed February 7, 2019, http://eng.mil.ru/en/structure/forces/cosmic.htm.

151 The Military Doctrine of the Russian Federation," Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland, press release, December 25, 2014, https://rusemb.org.uk/press/2029.

152 "Militarization, Weaponization, and the Prevention of an Arms Race," Reaching Critical Will, http://www.reachingcriticalwill.org/resources/fact-sheets/critical-issues/5448-outer-space.

153 Dipanjan Roy Chaudhury, "Russia Puts Onus on US for Early Outer Space Rules after India's Test," *Economic Times*, March 29, 2019, https://economictimes.indiatimes.com/news/defence/russia-puts-onus-us-for-early-outer-space-rules-after-indias-test/articleshow/68626644.cms?from=mdr.

154 Dara Massicot, "Anticipating a New Russian Military Doctrine in 2020: What It Might Contain and Why It Matters," War on the Rocks, September 9, 2019, https://warontherocks.com/2019/09/anticipating-a-new-russian-military-doctrine-in-2020-what-it-might-contain-and-why-it-matters/.

155 "Рогозин: Россия не использует спутники для повреждения космических аппаратов других стран," TASS, October 1, 2018, https://tass.ru/kosmos/5624853.

156 Jason Lemon, "Russia Will 'Respond' to 'New Threats' Created by Trump's Space Militarization, Russian Army Official Warns," *Newsweek*, March 4, 2019, https://www.newsweek.com/russia-respond-threats-trump-space-militarization-1350861.

157 "Putin Urges Greater Attention to Strengthening Orbital Group of Satellites," TASS, December 4, 2019, https://tass.com/science/1095757.

158 Asif A. Siddiqi, "The Soviet Co-Orbital Anti-Satellite System: A Synopsis," *Journal of the British Interplanetary Society* 50, no. 6 (1997): 225-40, http://faculty.fordham.edu/siddiqi/writings/p7_siddiqi_jbis_is_history_1997.pdf.

159 Anatoly Zak, "IS Anti-Satellite System," Russian Space Web, July 31, 2017, http://www.russianspaceweb.com/is.html.

160 Anatoly Zak, "Naryad Anti-Satellite System (14F11)," Russian Space Web, November 30, 2017, http://www.russianspaceweb.com/naryad.html.

161 Ibid.

162 Note: "PL-19" is a Western identifier (corresponding to the 19th system in its category observed from the Plesetsk Cosmodrome), while "Nudol" is a Russian identifier; Amanda Macias and Michael Sheetz, "Russia Conducted Another Successful Test of and Anti-satellite Missile, According to a Classified US Intelligence Report," CNBC, January 18, 2019, https://www.cnbc.com/2019/01/18/russia-succeeds-in-mobile-anti-satellite-missile-test-us-intelligence-report.html.

163 Bill Gertz, "Russia Flight Tests Anti-Satellite Missile," Washington Free Beacon, December 2, 2015, https://freebeacon.com/national-security/russia-conducts-successful-flight-test-of-anti-satellite-missile/.

164 "Russia's ASAT Development Takes Aim at LEO Assets," *Jane's Intelligence Review*, 2018, 1 https://www.janes.com/images/assets/591/81591/Russias_ASAT_development_takes_aim_at_LEO_assets.pdf.

165 Ibid.

166 "S-500 Prometheus," Missile Threat, CSIS, September 28, 2017, https://missilethreat.csis.org/defsys/s-500-prometheus/.

167 Mark B. Schneider, "Russian Nuclear Weapons Policy," RealClearDefense, April 28, 2017, https://www.realcleardefense.com/articles/2017/04/28/russian_nuclear_weapons_policy_111261.html.

168 Steve Lambakis, *Foreign Space Capabilities: Implications for U.S. National Security* (Fairfax, VA: National Institute Press, National Institute for Public Policy, 2017), http://www.nipp.org/wp-content/uploads/2017/09/Foreign-Space-Capabilities-pub-2017.pdf; "Russia Tests S-500 Air Defense System," Missile Threat, CSIS, September 28, 2017, https://missilethreat.csis.org/russia-successfully-tests-s-500-air-defense-system/; and Leonid Khayremdinov, "Обрести Навык Атак в Стратосфере," Красная Звезда, March 1, 2019, http://redstar.ru/obresti-navyk-atak-v-stratosfere/, quoted in Julian Cooper, "Russia's 'Invincible' Weapons: An Update," Changing Character of War Centre, March 27, 2019, http://www.ccw.ox.ac.uk/blog/2019/3/27/russias-invincible-weapons-an-update-by-julian-cooper.

169 "Russia's ASAT Development Takes Aim at LEO Assets," *Jane's Intelligence Review,* 1.

170 "Mikoyan-Gurevich MiG-31BM Foxhound," JetPhotos, September 14, 2018, https://www.jetphotos.com/photo/9074544; Amanda Macias, "A Never-before-seen Russian Missile Is Identified as an Anti-satellite Weapon and Will Be Ready for Warfare by 2022," CNBC, October 25, 2018, https://www.cnbc.com/2018/10/25/russian-missile-identified-as-anti-satellite-weapon-ready-by-2022.html.

171 James R. Clapper, "Worldwide Threat Assessment of the US Intelligence Community," Office of the Director of National Intelligence, February 9, 2016, 10, https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf.

172 Alexander Zudin, "Russia to Deploy Anti-satellite Weapon on MiG-31BM," *IHS Jane's Missiles and Rockets*, February 22, 2017.

173 "Mikoyan-Gurevich MiG-31BM Foxhound," JetPhotos; and Amanda Macias, "A Never-before-seen Russian Missile Is Identified as an Anti-satellite Weapon and Will Be Ready for Warfare by 2022."

174 Mike Wall, "'Very Abnormal' Russian Satellite Doesn't Seems So Threatening, Experts Say," Space.com, August 16, 2018, https://www.space.com/41511-weird-russian-satellite-not-so-abnormal.html.

175 Jonathan McDowell, "International Space Station," Jonathan's Space Report, No. 752, August 17, 2018, http://planet4589.org/space/jsr/back/news.752.txt.

176 Bart Hendrickx, "Russia Develops Co-orbital Anti-satellite Capability," *Jane's Intelligence Review*, September 27, 2018, 2.

177 Sandra Erwin, "Raymond calls out Russia for 'threatening behavior' in outer space," SpaceNews, February 10, 2020, https://spacenews.com/raymond-calls-out-russia-for-threatening-behavior-in-outer-space/.

178 Hendrickx, "Russia Develops Co-orbital Anti-satellite Capability," 3.

179 Bart Hendrickx, "OSINT Snapshot: New Russian satellites likely to have inspection role," *Jane's Intelligence Review*, July 25, 2019, 1; Bart Hendrickx, "Russia's Secret Satellite Builder," Space Review, May 6, 2019, https://www.thespacereview.com/article/3709/1.

180 "Orbital Launches of 2019," Gunter's Space Page, 2020, https://space.skyrocket.de/doc_chr/lau2019.htm; and Ministry of Defence of the Russian Federation, "Russian Aerospace Forces successfully launches Soyuz-2 lanch vehicle from Plesetsk Cosmodrome," Russian Federation, November 26, 2019, http://eng.mil.ru/en/news_page/country/more.htm?id=12263690@egNews.

181 Anatoly Zak, “Soyuz-2-1v Launches Classified Payload,” Russian Space Web, January 29, 2020, accessed on February 2, 2020, http://www.russianspaceweb.com/cosmos-2542.html.

182 Ibid.

183 Jonathan McDowell, Twitter post, January 31, 2020, 8:37 p.m., https://twitter.com/planet4589/status/1223420130576818176.

184 Michael Thompson, Twitter post, January 31, 2020, 11:40 p.m., https://twitter.com/M_R_Thomp/status/1223466202967760896.

185 Erwin, “Raymond calls out Russia.”

186 Hendrickx, “Russia Develops Co-orbital Anti-satellite Capability,” 1.

187 Ibid., 6.

188 Hendrickx, “Russia’s Secret Satellite Builder.”

189 “Космический аппарат ‹Луч› выведен на расчетную орбиту,” Aviation Explorer, September 29, 2014, https://www.aex.ru/news/2014/9/29/125060/.

190 Brian Weeden, “Dancing in the dark redux: Recent Russian rendezvous and proximity operations in space,” Space Review, October 5, 2015, http://www.thespacereview.com/article/2839/2.

191 Ibid.; Laurence Peter, “Russia Shrugs off US Anxiety over Military Satellite,” BBC News, October 20, 2015, https://www.bbc.com/news/world-europe-34581089.

192 “Luch (Olimp-K),” Gunter’s Space Page, 2019, https://space.skyrocket.de/doc_sdat/olimp-k.htm.

193 Thomas G. Roberts, “Unusual Behavior in GEO: Luch (Olymp-K),” Aerospace Security Project, CSIS, accessed March 01, 2020, https://aerospace.csis.org/data/unusual-behavior-in-geo-olymp-k/.

194 Vladimir Putin, “Presidential Address to the Federal Assembly,” (speech, Manezh Central Exhibition Hall, Moscow, Russia, March 1, 2018), http://en.kremlin.ru/events/president/news/56957.

195 Asif A. Siddiqi, “The Soviet Co-Orbital Anti-Satellite System: A Synopsis,” *Journal of the British Interplanetary Society* 50, no. 6 (1997), 225-40, http://faculty.fordham.edu/siddiqi/writings/p7_siddiqi_jbis_is_history_1997.pdf.

196 William R. Graham and Peter Vincent Pry, “Statement for the Record,” U.S. Congress, House, Committee on Homeland Security, Subcommittee on Oversight and Management Efficiency, October 12, 2017, 6, http://docs.house.gov/meetings/HM/HM09/20171012/106467/HHRG-115-HM09-Wstate-PryP-20171012.pdf; Jerry Emanuelson, “Soviet Test 184: The 1962 Soviet Nuclear EMP Tests over Kazakhstan,” FutureMscience LLC, http://www.futurescience.com/emp/test184.html; and ibid., 230.

197 “Transcript On Vienna Conference,” House Armed Services Committee, U.S. Congress, May 2, 1999, quoted in Peter Vincent Pry, “Nuclear EMP Attack Scenarios and Combined-Arms Cyber Warfare,” Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, July 2017, 3, https://michaelmabee.info/wp-content/uploads/2019/01/2017-Nuclear-Electromagnetic-Pulse-Attack-Scenarios-and-Combined-Arms-Cyber-Warfare.pdf.

198 Bart Hendrickx, “Self-Defense in Space: Protecting Russian Spacecraft from ASAT Attacks,” Space Review, July 16, 2018, https://www.thespacereview.com/article/3536/1.

199 A. Antonov et al., “История и перспективы развития низкотемпературных пиротехнических генераторов,” Известия Тульского государственного университета, 2016, https://cyberleninka.ru/article/n/istoriya-i-perspektivy-razvitiya-nizkotemperaturnyh-pirotehnicheskih-generatorov, quoted in ibid.

200 “Наука и Техника: Россия Создаст Лазер Для Подавления Разведки Противника,” Lenta.ru, August 8, 2010, http://lenta.ru/news/2010/08/19/laser.

201 Pavel Podvig, “Russia Has Been Testing Laser ASAT,” Russian Strategic Nuclear Forces, October 8, 2011, http://russianforces.org/blog/2011/10/russia_has_been_testing_laser.shtml.

202 “В РФ Разрабатывается Противоспутниковая Система РЭБ,” Военное Обозрение, April 25, 2017, https://topwar.ru/114285-v-rf-razrabatyvaetsya-protivosputnikovaya-sistema-reb.html, quoted in Patrick Tucker, “Russia Claims It Now Has Lasers To Shoot Satellites,” Defense One, February 26, 2018, https://www.defenseone.com/technology/2018/02/russia-claims-it-now-has-lasers-shoot-satellites/146243/.

203 Patrick Tucker, “Russia Claims It Now Has Lasers To Shoot Satellites,” Defense One, February 6, 2018, https://www.defenseone.com/technology/2018/02/russia-claims-it-now-has-lasers-shoot-satellites/146243/; “Источник узнал о перспективах создания в РФ нового самолета с лазерным оружием,” Interfax, February 25, 2018, translation by author, https://www.interfax.ru/russia/601331.

204 Vladimir Putin, “Presidential Address to the Federal Assembly.”

205 Anton Nikitin, “Боевые Лазеры «Пересвет» Заступили На Опытно-Боевое Дежурство,” Взгляд, December 5, 2018, https://vz.ru/news/2018/12/5/953800.html.

206 “Peresvet combat laser system,” Russian Ministry of Defense, YouTube video, 0:42, Russian Ministry of Defense, July 19, 2018, https://www.youtube.com/watch?v=ghDvDFb3lM0.

207 Iskander Batyrov, “Добьет Ли «Пересвет» До Цели,” Независимая, December 5, 2018, http://www.ng.ru/armies/2018-12-05/2_7456_target.html.

208 Vladimir Putin, “Presidential Address to the Federal Assembly,” (speech, Gostiny Dvor, Moscow, Russia, February 20, 2019), http://en.kremlin.ru/events/president/news/59863.

209 Julian Cooper, “Russia’s ‘Invincible’ Weapons: An Update,” Changing Character of War Centre, March 27, 2019, http://www.ccw.ox.ac.uk/blog/2019/3/27/russias-invincible-weapons-an-update-by-julian-cooper.

210 Center for Advanced Defense Studies (C4ADS), *Above Us Only Stars* (Washington, DC: March 2019), 3, https://www.c4reports.org/aboveusonlystars.

211 Dana Goward, “Mass GPS Spoofing Attack in Black Sea?” *Maritime Executive*, July 11, 2017, https://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea#gs.QGC4kZ8; Alexandra Coultrup, “GPS Jamming in the Arctic Circle,” Aerospace Security Project,

CSIS, April 4, 2019, https://aerospace.csis.org/data/gps-jamming-in-the-arctic-circle/; and ibid., 14.

212 "Russia Denies Role in Israeli Airport GPS Jamming," BBC News, June 27, 2019, https://www.bbc.com/news/technology-48786085; Thomas Nilsen, "Norway Tired of Russia's Electronic Warfare Troubling Civilian Navigation: 'Unacceptable and Risky'," *Barents Observer*, January 20, 2019, https://thebarentsobserver.com/en/security/2019/01/norway-tired-russian-military-gps-jamming-unacceptable-and-risky; and "Russia Denies Disrupting GPS Signals during Nato Arctic Exercises," *Guardian*, November 12, 2018, https://www.theguardian.com/world/2018/nov/12/russia-denies-blame-for-arctic-gps-interference.

213 Sergey Sukhankin, "Russian Electronic Warfare in Ukraine: Between Real and Imaginable," RealClearDefense, May 26, 2017, https://www.realcleardefense.com/articles/2017/05/26/russian_electronic_warfare_in_ukraine_111460.html; "It is official, Russian army deployed R-330Zh jammer in the battle of Debaltseve," Inform Napalm, May 14, 2016, https://informnapalm.org/en/r-330zh-jammer-battle-debaltseve/; and "Russian R-330Zh jammer detected 7 km from the contact line in Donbas," Inform Napalm, November 16, 2017, https://informsnapalm.org/en/russian-r-330zh-jammer-detected-7-km-from-the-contact-line-in-donbas/.

214 Elias Groll, "Spy Planes, Signal Jammers, and Putin's High-Tech War in Syria," *Foreign Policy*, October 6, 2015, http://foreignpolicy.com/2015/10/06/spy-planes-signal-jammers-and-putins-high-tech-war-in-syria; and David Stupples, "How Syria is becoming a test bed for high-tech weapons of electronic warfare," *The Conversation*, October 8, 2015, https://theconversation.com/how-syria-is-becoming-a-test-bed-for-high-tech-weapons-of-electronic-warfare-48779.

215 C4ADS, *Above Us Only Stars*, 3.

216 Ibid., 14.

217 Dmitry Krilov, "Кремль Продолжит Искажать," Газета.ru, December 19, 2016, https://www.gazeta.ru/auto/2016/12/16_a_10430909.shtml.

218 "Moscow Taxi Users Confusion amid GPS Meddling Claims," BBC News, January 10, 2018, https://www.bbc.com/news/technology-42633024.

219 "St. Petersburg Drivers Report Strange GPS Problems in City Center," *Moscow Times*, December 27, 2016, https://www.themoscowtimes.com/2016/12/27/drivers-in-st-petersburg-report-gps-problems-in-city-center-a56653.

220 Coultrup, "GPS Jamming in the Arctic Circle."

221 Mark Episkopos, "Russia Jammed GPS Signals During a NATO Military Exercise. That's a Really Big Deal.", *National Interest*, December 1, 2018, https://nationalinterest.org/blog/buzz/russia-jammed-gps-signals-during-nato-military-exercise-thats-really-big-deal-37682; and Harald Tomassen and Allan Klo, "Monterer Målestasjon for å Oppdage GPS-Jamming," NRK, March 11, 2019, https://www.nrk.no/finnmark/monterer-malestasjon-for-a-oppdage-gps-jamming-1.14467017.

222 "Ships Fooled in GPS Spoofing Attack Suggest Russian Cyberweapon," *New Scientist*, August 10, 2017, https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/.

223 C4ADS, *Above Us Only Stars*, 20.

224 Ibid., 3.

225 Ibid., 18, 23.

226 Patrick Tucker, "US and Russia Regard Each Other Warily in the Baltic and Black Seas," Defense One, January 24, 2019, https://www.defenseone.com/threats/2019/01/us-and-russia-eye-each-other-warily-baltic-and-black-seas/154404/; and Andrew Roth, "Kerch strait confrontation: what happened and why does it matter?," *Guardian*, November 27, 2018, https://www.theguardian.com/world/2018/nov/27/kerch-strait-confrontation-what-happened-ukrainian-russia-crimea.

227 Brian Wang, "Russia will place GPS jammers on 250,000 cellphone towers to reduce enemy cruise missile and drone accuracy in the event of large scale conventional war," Next Big Future, October 18, 2016, https://www.nextbigfuture.com/2016/10/russia-will-place-gps-jammers-on-250000.html.

228 "Latest jamming system arrives for electronic warfare troops in central Russia," TASS, November 13, 2019, https://tass.com/defense/1088451.

229 Michael Peck, "Why Russia's New Anti-Satellite Plane Is Very Bad Idea," National Interest, October 20, 2019, https://nationalinterest.org/blog/buzz/why-russias-new-anti-satellite-plane-very-bad-idea-89716.

230 Bart Hendrickx, "Ekipazh: Russia's top-secret nuclear-powered satellite," Space Review, October 7, 2019, https://www.thespacereview.com/article/3809/1.

231 James Landale, "Russia Cyber-Plots: US, UK and Netherlands Allege Hacking," BBC News, October 4, 2018, https://www.bbc.com/news/world-europe-45746837.

232 Estonian Foreign Intelligence Service, *International Security and Estonia* (Tallinn: 2018), 53, https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf; Ellen Nakashima, "Russian hacker group exploits satellites to steal data, hide tracks," *Washington Post*, September 9, 2015, https://www.washingtonpost.com/world/national-security/russian-hacker-group-exploits-satellites-to-steal-data-hide-tracks/2015/09/08/c59fa7cc-5657-11e5-b8c9-944725fcd3b9_story.html?utm_term=.43d8b0ed4c7f; and "Turla: Spying tool targets governments and diplomats," Symantec Security Response, August 7, 2014, https://www.symantec.com/connect/blogs/turla-spying-tool-targets-governments-and-diplomats.

233 Jack Stubbs and Christopher Bing, "Hacking the Hackers: Russian Group Hijacked Iranian Spying Operation, Officials Say," Reuters, October 21, 2019, https://www.reuters.com/article/us-russia-cyber/hacking-the-hackers-russian-group-hijacked-iranian-spying-operation-officials-say-idUSKBN1X00AK.

234 Gordon Corera, "How France's TV5 Was Almost Destroyed by 'Russian Hackers'," BBC News, October 10, 2016, https://www.bbc.com/news/technology-37590375.

235 Natasha Lomas, "UK Says Russia's GRU Was behind a Spate of Chaotic Cyber Attacks between 2015 and 2017," TechCrunch, October 4, 2018, https://techcrunch.com/2018/10/04/uk-says-russias-gru-was-behind-a-spate-of-chaotic-cyber-attacks-between-2015-and-2017/.

236 Damien McGuinness, "How a cyber attack transformed Estonia," BBC News, April 27, 2017, http://www.bbc.com/news/39655415; Sergey Sukhankin, "Russian Electronic Warfare in Ukraine: Between Real and Imaginable," RealClearDefense, May 26, 2017, https://www.realcleardefense.com/articles/2017/05/26/russian_electronic_warfare_in_ukraine_111460.html; David E. Sanger, "Putin Ordered 'Influence Campaign' Aimed at U.S. Election, Report Says," *New York Times*, January 6, 2017, https://www.nytimes.com/2017/01/06/us/politics/russia-hack-report.html; and James Landale, "Russia Cyber-Plots: US, UK and Netherlands Allege Hacking," BBC News, October 4, 2018, https://www.bbc.com/news/world-europe-45746837.

237 Jens Stoltenberg, "Nato Will Defend Itself," *Prospect Magazine*, December 27, 2019, https://www.prospectmagazine.co.uk/world/nato-will-defend-itself-summit-jens-stoltenberg-cyber-security; and Michael Imeson, "Russia Cyber Aggression Fuels Tensions with West," *Financial Times*, October 14, 2019, https://www.ft.com/content/0aa7a6e0-ca52-11e9-af46-b09e8bfe60c0.

238 James Landale, "Russia Cyber-Plots: US, UK and Netherlands Allege Hacking," BBC News, October 4, 2018, https://www.bbc.com/news/world-europe-45746837.

239 Todd Harrison, Kaitlyn Johnson, and Thomas G. Roberts, *Space Threat Assessment 2018* (Washington, DC: CSIS, April 2018), https://aerospace.csis.org/wp-content/uploads/2018/04/Harrison_SpaceThreatAssessment_FULL_WEB.pdf; Todd Harrison, Kaitlyn Johnson, and Thomas G. Roberts, *Space Threat Assessment 2019* (Washington, DC: CSIS, April 2019), https://aerospace.csis.org/wp-content/uploads/2019/04/SpaceThreatAssessment2019-compressed.pdf.

IRAN

240 Thomas G. Roberts, *Spaceports of the World* (Washington, DC: CSIS, January 2020) https://aerospace.csis.org/data/spaceports-of-the-world/.

241 Mike Pompeo, "United States Imposes New Sanctions Designations on Iran's Space Program as Tehran Continues to Use Civilian Space Agencies to Advance Its Ballistic Missile Programs," U.S. Department of State, press release, September 13, 2019, https://www.state.gov/united-states-imposes-new-sanctions-designations-on-irans-space-program-as-tehran-continues-to-use-civilian-space-agencies-to-advance-its-ballistic-missile-programs/.

242 David E. Sanger and William J. Broad, "U.S. Accuses Iran of Using Space Launch as Cover for Missile Program," *New York Times*, January 4, 2019, https://www.nytimes.com/2019/01/03/world/middleeast/iran-spacecraft-pompeo.html.

243 Kevjn Lim and Gil Baram, "Iran Is Mastering the Final Frontier," *Foreign Policy*, March 14, 2019, https://foreignpolicy.com/2019/03/14/iran-is-mastering-the-final-frontier/.

244 Fredrik Dahl, "Iran Launches Satellite; U.S. Expresses Concern," Reuters, February 3, 2009, https://www.reuters.com/article/us-iran-satellite-idUSTRE5120NN20090203.

245 "Iran 'Sends Monkey to Space for Second Time'," BBC News, December 14, 2013, https://www.bbc.com/news/world-middle-east-25378313.

246 Farzon Nadimi, "Iran's Space Program Emerges from Dormancy," Washington Institute for Near East Policy, August 1, 2017, https://www.washingtoninstitute.org/policy-analysis/view/irans-space-program-emerges-from-dormancy.

247 "Iran Missile Sites," CIA, n.d. https://www.cia.gov/library/abbottabad-compound/9B/9BF2B1E1B6F60BF4889BE25391570BEB_iran_missile_sites.pdf.

248 "Iran," Zarya, February 11, 2012, https://www.zarya.info/Diaries/Iran/Iran.php.

249 "Russia Signs Deal to Build & Launch Iran Satellites," Iran Times, May 14, 2014, http://iran-times.com/russia-signs-deal-to-build-launch-iran-satellites/.

250 Defense Intelligence Agency, *Iran Military Power* (Washington, DC: 2019), https://www.dia.mil/Portals/27/Documents/News/Military Power Publications/Iran_Military_Power_LR.pdf; and Daniel R. Coats, "Worldwide Threat Assessment of the US Intelligence Community," Office of the Director of National Intelligence, February 13, 2018, p. 10, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

251 Stephen M. McCall, "Iran's Ballistic Missile and Space Launch Programs," Congressional Research Service, January 9, 2020, https://fas.org/sgp/crs/nuke/IF10938.pdf.

252 "Iran Announces Security-Oriented 'Space Tracking Center'," RT International, June 9, 2013, https://www.rt.com/news/iran-space-monitoring-center-429/.

253 "Iran Claims To Have SSA Radar Capable of Detecting Satellites in LEO," Spacewatch, 2018, https://spacewatch.global/2018/12/iran-claims-to-have-ssa-radar-capable-of-detecting-satellites-in-leo/.

254 "Missiles of Iran," Missile Threat, CSIS, Accessed February 5, 2020, https://missilethreat.csis.org/country_tax/iran/.

255 "Simorgh," Missile Threat, CSIS, June 15, 2018, https://missilethreat.csis.org/missile/simorgh/.

256 Tyler Rodgers, "Iran's Simorgh Rocket Test in Perspective," Arms Control Association, January 17, 2017, https://www.armscontrol.org/blog/2017-07-27/iran-simorgh-rocket-test-in-perspective.

257 Geoff Brumfiel, "Iranian Rocket Launch Ends In Failure, Imagery Shows," NPR, August 29, 2019, https://www.npr.org/2019/08/29/755406765/iranian-rocket-launch-ends-in-failure-images-show; Stephen Clark, "Second Iranian Satellite Launch Attempt in a Month Fails," Spaceflight Now, February 11, 2019, https://spaceflightnow.com/2019/02/11/second-iranian-satellite-launch-attempt-in-a-month-fails/; and Geoff Brumfiel, "Satellite Imagery Suggests 2nd Iranian Space Launch Has Failed," NPR, February 6, 2019, https://www.npr.org/2019/02/06/692071812/satellite-imagery-suggests-second-iranian-space-launch-has-failed.

258 "Iran Space Agency to Launch Three Satellites by March 2020," Financial Tribune, August 25, 2019, https://financialtribune.com/articles/sci-tech/99569/iran-space-agency-to-launch-three-satellites-by-march-2020.

259 Geoff Brumfiel, "Iranian Rocket Launch Ends In Failure, Imagery Shows."

260 Geoff Brumfiel, "Trump Tweets Sensitive Surveillance Image Of Iran," NPR, August 30, 2019, https://www.npr.org/2019/08/30/755994591/

president-trump-tweets-sensitive-surveillance-image-of-iran; and Donald Trump, Twitter Post, August 30, 2019, 1:44 pm, https://twitter.com/realDonaldTrump/status/1167493371973255170

261 Matthew Lee, "US Hits Iran Space Agency with Sanctions over Missile Work," Associated Press, September 4, 2019, https://apnews.com/99a41d1896c94d9e967e581b3c2e2d83.

262 "Iran-related Designations; Non-proliferation Designations; Kingpin Act Designations Update," U.S. Department of the Treasury, September 3, 2019, https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20190903_33.aspx.

263 MJ Azari Jahromi, Twitter Post, January 29, 2020, 1:26 am, https://twitter.com/azarijahromi/status/1222405725651075072

264 2379, "Iran Makes Six Satellites to Put into Orbit," IRNA English, January 26, 2020, https://en.irna.ir/news/83648264/Iran-makes-six-satellites-to-put-into-orbit.

265 Amir Vahdat and Jon Gambrell, "Iran Again Fails to Put Satellite into Orbit amid US Worries," Associated Press, February 9, 2020, https://apnews.com/7c8247674c294c23d408b034e9d4ee5a?utm_campaign=SocialFlow&utm_source=Twitter&utm_medium=AP.

266 "Committee on the Peaceful Uses of Outer Space: Membership Evolution," United Nations Office for Outer Space Affairs, https://www.unoosa.org/oosa/en/ourwork/copuos/members/evolution.html; and "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial bodies," U.S. Department of State, Accessed February 5, 2020, https://2009-2017.state.gov/t/isn/5181.htm#signatory.

267 Parvis Tarikhi, "More Significant Role for Iran's Space Administration," Parviztarikhi's Blog, November 22, 2010, https://parviztarikhi.wordpress.com/features-2/more-significant-role-for-iran's-space-administration/.

268 "ایران فضایی سازمان," 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.

269 "Iran Space Research Center," Iran Watch, October 31, 2019, https://www.iranwatch.org/iranian-entities/iran-space-research-center; and "Sharif University of Technology," Iran Watch, November 18, 2019, https://www.iranwatch.org/iranian-entities/sharif-university-technology.; and "Iran Enjoys High-Tech in Building Space-Based Parks," IRNA English, September 29, 2019, https://en.irna.ir/news/83496207/Iran-enjoys-high-tech-in-building-space-based-parks.

270 Stephen Lambakis, *Foreign Space Capabilities: Implications for U.S. National Security* (Fairfax, VA: National Institutes Press, August 2017), 31, https://www.nipp.org/wp-content/uploads/2017/09/Foreign-Space-Capabilities-pub-2017.pdf.

271 Geoff Brumfiel, "Iran Is Preparing A Launch. But Is It For A Space Rocket Or A Missile?" NPR, January 14, 2019, https://www.npr.org/2019/01/14/684467347/iran-is-preparing-a-launch-but-is-it-for-a-space-rocket-or-a-missile.

272 "آفتاب اخبار. "اختصاص ۳ هزار و ۹۶۰ میلیارد تومان برای سازمان فضایی ایران," Aftabir.com, March 26, 2010, https://www.aftabir.com/news/view/2008/feb/20/c2c1203499802_economy_marketing_business_information_technology_mobile.php.

273 "Cuts and Extensions in Iran's ICT 2017/18 Budget," *Financial Tribune*, December 13, 2016, https://web.archive.org/web/20161220150555/https://financialtribune.com/articles/sci-tech/55397/cuts-and-extensions-in-irans-ict-201718-budget.

274 Jennifer Chandler, "Decoding Iran's defence spending: pitfalls and new pointers," International Institute for Strategic Studies, November 13, 2018, https://www.iiss.org/blogs/military-balance/2018/11/decode-iran-defence-spending.

275 "Iran Attack: How Strong Is Iran's Military?" BBC News, January 9, 2020, https://www.bbc.com/news/world-middle-east-50982743.

276 "Shahab-3," Missile Threat, CSIS, August 9, 2016, https://missilethreat.csis.org/missile/shahab-3/.

277 Robert Einhorn, Vann H Van Diepen, and Kate Hewitt, *Constraining Iran's Missile Capabilities* (Washington, DC: Brookings, March 2019), https://www.brookings.edu/wp-content/uploads/2019/03/FP_20190321_missile_program_WEB.pdf.

278 Tom O'Connor, "U.S. Warns 'Iran Has the Largest Ballistic Missile Force in the Middle East' and Can Target Europe," *Newsweek*, December 13, 2018, https://www.newsweek.com/us-iran-missile-force-middle-east-target-europe-1255834.

279 "Iran Opens New Space-Tracking Center," RadioFreeEurope/RadioLiberty, June 9, 2013, https://www.rferl.org/a/iran-space-tracking-center/25011651.html.

280 Michael Peck, "Bad News for Israel: Iran Has a New Missile," *National Interest*, November 1, 2019, https://nationalinterest.org/blog/buzz/bad-news-israel-iran-has-new-missile-92556; and Jeremey Binnie, "Iran displays guidance for artillery rockets," *Jane's Defence Weekly*, October 4, 2019, https://www.janes.com/article/91703/iran-displays-guidance-upgrade-for-artillery-rockets.

281 Ian Williams, "When Iran Attacks," Missile Threat, CSIS, February 4, 2020, https://missilethreat.csis.org/when-iran-attacks/.

282 "Missiles of Iran." Missile Threat, CSIS, Accessed February 5, 2020. https://missilethreat.csis.org/country_tax/iran/.

283 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.

284 "Iran's Nuclear Program Timeline and History," Nuclear Threat Initiative, last updated January 2020, https://www.nti.org/learn/countries/iran/nuclear/

285 Ibid.

286 United Against a Nuclear Iran, *Iran & North Korea - Nuclear Proliferation Partners* (New York, NY: February 2019), https://www.unitedagainstnuclearіran.com/north-korea-iran; and Josh Rogin and Eli Lake, "Iran and North Korea: The Nuclear 'Axis of Resistance'," The Daily Beast, January 31, 2014, https://www.thedailybeast.com/iran-and-north-korea-the-nuclear-axis-of-resistance.

287 Zachary Laub and Kali Robinson, "What Is the Status of the Iran Nuclear Agreement?" Council on Foreign Relations, last updated January 7, 2020, https://www.cfr.org/backgrounder/what-status-iran-nuclear-agreement.

288 John Haltiwanger, "Here's What's in the 2015 Nuclear Deal with Iran That the Country Withdrew from amid Heightened Tensions with the US," Business Insider, January 14, 2020, https://www.businessinsider.com/iran-nuclear-deal-explained.

289 Holly Ellyatt, "Europe Stands by Iran Nuclear Deal for Now, Defying US Calls to Abandon It," CNBC, January 13, 2020, https://www.cnbc.com/2020/01/13/jcpoa-europe-stands-by-iran-nuclear-deal.html.

290 Uri Friedman, "A New Nuclear Era Is Coming," The Atlantic, January 9, 2020, https://www.theatlantic.com/politics/archive/2020/01/soleimani-iran-north-korea-new-nuclear-age/604618/.

291 Safa Haeri, "Cuba blows the whistle on Iranian jamming," *Asia Times*, August 22, 2003, http://www.atimes.com/atimes/Middle_East/EH22Ak03.html.

292 Small Media Foundation, *Satellite Jamming in Iran: A War Over Airwaves* (London, UK: Small Media Foundation, 2012), 21, https://smallmedia.org.uk/sites/default/files/Satellite%20Jamming.pdf.

293 Yeganeh Torbati, "Iran says capable of jamming foes' communication systems," Reuters, January 15, 2013, https://in.reuters.com/article/iran-military/iran-says-capable-of-jamming-foes-communication-systems-idINDEE90E0DF20130115.

294 Michel de Rosen, "Letter to Eutelsat Regarding Iranian Government's jamming of satellite broadcasts," Human Rights Watch, June 25, 2010, https://www.hrw.org/news/2010/06/25/letter-eutelsat-regarding-iranian-governments-jamming-satellite-broadcasts.

295 Ibid.

296 Regan Doherty, "Iran Jamming Al Jazeera Broadcasts: Document," Reuters, January 10, 2012, https://www.reuters.com/article/us-iran-jazeera/iran-jamming-al-jazeera-broadcasts-document-idUSTRE80918520120110.

297 Robert Briel, "Syria in Frame on Eutelsat Jamming," Broadband TV News, October 22, 2012, https://www.broadbandtvnews. com/2012/10/22/syria-believed-to-jam-eutelsat/.

298 "London-Based Persian TV To Lodge Complaint Against Iran For Satellite Jamming." Radio Farda, November 23, 2019, https://en.radiofarda.com/a/london-based-persian-tv-to-lodge-complaint-against-iran-for-satellite-jamming-/30288280.html.

299 Peterson and Faramarzi, "Exclusive: Iran hijacked U.S. drone, says Iranian engineer."

300 Lee Feeran, "Obama: Hey Iran, Can We Get Our Drone Back?" ABC News, December 12, 2011, https://abcnews.go.com/Blotter/obama-asks-iran-rq-170-sentinel-drone-back/story?id=15140133.

301 "2019-012-Persian Gulf, Strait of Hormuz, Gulf of Oman, Arabian Sea, Red Sea-Threats to Commercial Vessels by Iran and Its Proxies." MARAD, July 8, 2019, https://www.maritime.dot.gov/content/2019-012-persian-gulf-strait-hormuz-gulf-oman-arabian-sea-red-sea-threats-commercial-vessels.

302 Reuters and *Haaretz*, "Iran Reportedly Jamming Ships' GPS in Attempt to Trick Them Into Iranian Waters for Seizure," *Haaretz*, August 8, 2019, https://www.haaretz.com/middle-east-news/iran/iran-reportedly-jamming-ships-gps-in-attempt-to-trick-them-into-iranian-waters-1.7652352.

303 Tzvi Joffre,"U.S. Warns of GPS Interference, Communications Spoofing in Persian Gulf." *Jerusalem Post*, August 8, 2019, https://www.jpost.com/Middle-East/US-warns-of-GPS-interference-communications-spoofing-in-Persian-Gulf-597998.

304 Tracy Cozzens, "Iran jams CPS on ships in Strait of Hormuz," GPS World, August 9, 2019, https://www.gpsworld.com/iran-jams-gps-on-ships-in-strait-of-hormuz/.

305 Seth J. Frantzman, "Iran Claims to Pioneer New Electronic Warfare Unit," *Jerusalem Post*, July 7, 2019, https://www.jpost.com/Middle-East/Iran-claims-to-pioneer-new-electronic-warfare-unit-594858.

306 "IRGC Unveils Military Communication System - Defense News," Tasnim News Agency, July 7, 2019, https://www.tasnimnews.com/en/news/2019/07/07/2048683/irgc-unveils-military-communication-system.

307 Alain Henry de Frahan, "Iran unveiled armored vehicle, jamming system, drones, smart robot and more," Army Recognition, October 4, 2019, https://www.armyrecognition.com/october_2019_global_defense_security_army_news_industry/iran_unveiled_armored_vehicle_jamming_system_drones_smart_robot_and_more.html; and Shi Yinglun, "Iran Unveils New Homemade Military Gears: Report," Xinhua, October 3, 2019, http://www.xinhuanet.com/english/2019-10/03/c_138446473.htm.

308 "New Prototype 'Farpad' UAV given to Military Units," IRNA English, October 30, 2019, https://en.irna.ir/news/83535778/New-prototype-Farpad-UAV-given-to-military-units; and "Iran's New Hand-launched Drone has Electronic Warfare Capability," DefenseWorld.net, October 31, 2019, https://www.defenseworld.net/news/25749/Iran_s_New_Hand_launched_Drone_has_Electronic_Warfare_Capability#.XjqAGxdyKiRu.

309 Dorothy Denning, "Iran's Cyber Warfare Program Has Reached a Critical Point," *Newsweek*, December 12, 2017, https://www.newsweek.com/irans-cyber-warfare-program-now-major-threat-united-states-745427.

310 Keith Breene, "Who Are the Cyberwar Superpowers?" World Economic Forum, May 4, 2016, https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/.

311 James A. Lewis, "Iran and Cyber Power," CSIS, *Commentary,* June 25, 2019, https://www.csis.org/analysis/iran-and-cyber-power; and Seth G. Jones, *Containing Tehran*, (Washington, DC: CSIS, January 2020), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/200110_Jones_ContainingIran_WEB_v2.pdf?MiOEbYgRpCYPIeM5sivMoNWJIhFDxrN5.

312 Ibid

313 Collin Anderson and Karim Sadjadpour, Iran's Cyber Threat: Espionage, Sabotage, and Revenge (Washington, DC: Carnegie Endowment for International Peace, January 4, 2018) 47, https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf.

314 "The Invisible U.S.-Iran Cyber War," U.S. Institute for Peace, *The Iran Primer*, updated January 7, 2020, https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war.

315 Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times*, October 11, 2012, https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

316 "The Invisible U.S.-Iran Cyber War," U.S. institute for Peace.

317 "CISA Statement on Iranian Cybersecurity Threats," Department of Homeland Security, October 30, 2019, https://www.dhs.gov/news/2019/06/22/cisa-statement-iranian-cybersecurity-threats.

318 Brian Fung, "Hacking Attempts Originating in Iran Nearly Triple Following Soleimani Strike, Researchers Say," CNN, January 9, 2020, https://www.cnn.com/2020/01/08/tech/iran-hackers-soleimani/index.html.

NORTH KOREA

319 Thomas G. Roberts, *Spaceports of the World* (Washington, DC: CSIS, March 2019), https://www.csis.org/analysis/spaceports-world.

320 "A Conversation with General John Hyten, Vice Chairman of the Joint Chiefs of Staff" (public event, CSIS, Washington, DC, January 17, 2020), https://www.csis.org/events/conversation-general-john-hyten-vice-chairman-joint-chiefs-staff. Filmed [January 17, 2020]. Youtube video, 18:38. Posted [January 17, 2020], https://www.youtube.com/watch?v=d1v9fpcfi78.

321 "Taepodong-2 (Unha-3)," Missile Threat, CSIS, August 8, 2016, last modified June 15, 2018, https://missilethreat.csis.org/missile/taepodong-2/.

322 Elizabeth Shim, "North Korea Defends ''Peaceful'' Satellite Launches, Report Says," UPI, January 6, 2020, https://www.upi.com/Top_News/World-News/2020/01/06/North-Korea-defends-peaceful-satellite-launches-report-says/7681578311980/.

323 Robert E. Mccoy, "What are the real purposes of Pyongyang's new satellites?" *Asia Times*, December 19, 2017, http://www.atimes.com/article/real-purposes-pyongyangs-new-satellites/.

324 Eric Talmadge, "AP Exclusive: North Korea Hopes to Plant Flag on the Moon," Associated Press, August 4, 2016, https://apnews.com/88fa176909dec40b299658a34b489dc1a/AP-Exclusive:-North-Korea-hopes-to-plant-flag-on-the-moon.

325 "North Korean Missile Launches & Nuclear Tests: 1984-Present," Missile Threat, CSIS, December 3, 2019, https://missilethreat.csis.org/north-korea-missile-launches-1984-present/.

326 Barbara Starr and Zachary Cohen, "Satellite Imagery Shows Activity at Critical North Korean Missile Site," CNN, January 26, 2020, https://www.cnn.com/2020/01/26/politics/north-korea-satellite-imagery-missile-site/index.html.

327 Joseph Bermudez, Victor Cha, and Dana Kim, "December 2019 Update: Tonghae Satellite Launching Ground," Beyond Parallel, CSIS, December 17, 2019, https://beyondparallel.csis.org/december-2019-update-tonghae-satellite-launching-ground/.

328 Alex Ward, "Why North Korea's restored rocket site isn't cause for worry — yet," Vox, March 7, 2019, https://www.vox.com/2019/3/7/18254589/north-korea-rocket-site-launch-space-trump-vietnam.

329 "North Korea's Sohae Satellite Launching Station: Post-Engine Test Activity Observed," 38 North, December 17, 2019, https://www.38north.org/2019/12/sohae121619/.

330 Spokesman for Academy of Defence Science of DPRK Issues Statement," KCNA Watch, December 15, 2019, https://kcnawatch.org/newstream/1576486826-622749970/spokesman-for-academy-of-defence-science-of-dprk-issues-statement/; "Statement of Spokesman for Academy of National Defence Science Issued," KCNA Watch, December 9, 2019, https://kcnawatch.org/newstream/1575882057-292334499/statement-of-spokesman-for-academy-of-national-defence-science-issued/.

331 Heekyong Yang, "North Korea Conducts New Test at Rocket Site, Aims to 'Overpower U.S. Nuclear Threats'," Reuters, December 14, 2019, https://www.reuters.com/article/us-northkorea-missiles/north-korea-conducts-new-test-at-rocket-site-aims-to-overpower-us-nuclear-threats-idUSKBN1YI05E.

332 Weeden and Samson, eds., *Global Counterspace Capabilities* (Washington, DC: Secure World Foundation, April 2019), 5–1, https://swfound.org/media/206408/swf_global_counterspace_april2019_web.pdf.

333 "North Korea Finishes Advanced Recon Satellite," Space Daily, December 27, 2017, https://www.spacedaily.com/reports/North_Korea_finishes_advanced_recon_satellite_999.html.

334 "Stronger Rules Must Guarantee Outer Space Remains Conflict-Free, First Committee Delegates Stress, Calling for New Laws to Hold Perpetrators Accountable," United Nations, October 17, 2017, https://www.un.org/press/en/2017/gadis3583.doc.htm.

335 "KCNA Report on DPRK's Accession to International Space Treaty and Convention," KCNA Watch, March 12, 2009, https://kcnawatch.org/newstream/1451888128-747969205/kcna-report-on-dprks-accession-to-international-space-treaty-and-convention/.

336 "Seventh Session of 12th SPA of DPRK Held," KCNA, April 1, 2013, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&Asource=web&cd=1&ved=2ahUKEwj-3cPX3dnnAhVDKH0KHffLCg0QFjAAegQIARAB&url=http%3A%2F%2Fwww.kcna.co.jp%2Fitem%2F2013%2F201304%2Fnews01%2F20130401-23ee.html&usg=AOvVaw10gT0npAmRPomIQ9hBgp6b.

337 Sofia Lotto Persio, "North Korea Is Reaching for the Stars with Plans to Conquer Space," *Newsweek*, October 30, 2017, https://www.newsweek.com/star-wars-north-koreas-unveils-5-year-plan-conquer-space-695896Y.

338 "DPRK Delegate Speaks at UNGA Session." KCNA Watch, October 21, 2017, https://kcnawatch.org/newstream/1508666429-52873364/dprk-delegate-speaks-at-unga-session/.

339 Morris Jones, "North Korea's Space Program Aims Higher," Lowy Institute, *Interpreter,* October 31, 2017, https://www.lowyinstitute.org/the-interpreter/north-korea-space-program-aims-higher.

340 "Space Will Bring Greater Well-Being to Mankind: Minju Joson," KCNA Watch, April 12, 2017, https://kcnawatch.org/newstream/273151/space-will-bring-greater-well-being-to-mankind-minju-joson/.

341 "'Sanctions Won't Stop Our Space Race': North Korea Sets Sights on the Moon," *Guardian*, August 4, 2016, https://www.theguardian.com/world/2016/aug/04/sanctions-wont-stop-our-space-race-north-korea-sets-sights-on-the-moon.

342 Ibid.; Persio, "North Korea Is Reaching for the Stars with Plans to Conquer Space."

343 "No Dong 1," Missile Threat, CSIS, June 15, 2018, https://missilethreat.csis.org/missile/no-dong/; and Wright, Grego, and Gronlund, *The Physics of Space Security*, 77.

344 National Coordination Office for Space-Based Positioning, Navigation, and Timing, "Control Segment."

345 Wright, Grego, and Gronlund, *The Physics of Space Security*, 125-130.

346 Elise Hu, "North Korea Claims Successful Hydrogen Bomb Test." NPR, September 3, 2017, https://www.npr.org/sections/thetwo-way/2017/09/03/523913820/north-korea-possibly-conducts-sixth-nuclear-test-south-korea-says.

347 Emma Bowman, "North Korea Brandishes What It Says Is A Missile-Ready H-Bomb." NPR, September 3, 2017, https://www.npr.org/sections/thetwo-way/2017/09/03/548201793/north-korea-brandishes-what-it-says-is-a-missile-ready-h-bomb.

348 "Kim Jong Un Advances Tasks for Effecting Drastic Turn in Implementing Decision of 7th Congress of WPK," KCNA Watch, January 1, 2017, https://kcnawatch.org/newstream/1483266680-358842164/kim-jong-un-advances-tasks-for-effecting-drastic-turn-in-implementing-decision-of-7th-congress-of-wpk/.

349 "Report on 5th Plenary Meeting of 7th C.C., WPK," KCNA Watch, January 1, 2020, https://kcnawatch.org/newestream/1577869229-462791867/report-on-5th-plenary-meeting-of-7th-c-c-wpk/.

350 Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack,"*Assessing the Threat from Electromagnetic Pulse (EMP)*" (Washington, DC: Department of Defense, July 2017), http://www.firstempcommission.org/uploads/1/1/9/5/119571849/executive_report_on_assessing_the_threat_from_emp_-_final_april2018.pdf.

351 Mun Dong Hui, "North Korean Propaganda Promotes EMP Attacks Using Nuclear Weapons," Daily NK, January 17, 2020, https://www.dailynk.com/english/north-korean-propaganda-promotes-emp-attacks-using-nuclear-weapons/.

352 Bureau of Arms Control, Verification and Compliance, "Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water," U.S. Department of State, https://www.state.gov/t/isn/4797.htm.

353 "N. Korea's jamming of GPS signals poses new threat: defense minister," Yonhap News Agency, October 5, 2010, http://english.yonhapnews.co.kr/national/2010/10/05/67/0301000000AEN20101005005900315F.HTML.

354 Choe Sang-Hun, "South Korea: North accused of sending jamming signals to disrupt GPS," *New York Times,* May 3, 2012, http://www.nytimes.com/2012/05/03/world/asia/south-korea-accused-north-accused-of-jamming-signals.html.

355 Ian Wood and Stella Kim, "North Korea Jams GPS Signals to Fishing Boats: South," NBC News, April 1, 2016, https://www.nbcnews.com/news/world/north-korea-jams-gps-signals-fishing-boats-south-n548986.

356 "South Korea tells U.N. that North Korea GPS jamming threatens boats, planes," Reuters, April 11, 2016, https://www.reuters.com/article/us-northkorea-southkorea-gps/south-korea-tells-u-n-that-north-korea-gps-jamming-threatens-boats-planes-idUSKCN0X81SN.

357 Mun Dong Hui, "North Korean Propaganda Promotes EMP Attacks Using Nuclear Weapons," Daily NK, November 23, 2018, https://www.dailynk.com/english/north-korean-propaganda-promotes-emp-attacks-using-nuclear-weapons/.

358 "Massive GPS Jamming Attack by North Korea," GPS World, May 8, 2012, http://gpsworld.com/massive-gps-jamming-attack-by-north-korea/.

359 Catherine Dill et all., "On the Trail of the Tae Yang," Royal United Services Institute for Defence and Security Studies and Middlebury Institute of International Studies at Monterey, James Martin Center for Nonproliferation Studies, 2019, https://rusi.org/sites/default/files/project_sandstone_on_the_trail_of_the_tae_yang_final_for_web_4.pdf.

360 Benjamin Katzeff Silberstein, Tereza Novotna, and Kenneth B. Dekleva, "North Korea's Koryolink: Built for Surveillance and Control" 38 North, August 12, 2019, https://www.38north.org/2019/07/mwilliams072219/.

361 CrowdStrike. *2019 Global Threat Report: Adversary Tradecraft and the Importance of Speed* (Sunnyvale, CA: 2019), https://www.lufsec.com/wp-content/uploads/2019/06/CrowdStrike_GTR_2019.pdf.

362 Kim Jaewon, "A Cybersecurity Defector Warns of North Korea's 'Hacker Army'," *Nikkei Asian Review*, May 25, 2017, https://asia.nikkei.com/Politics/A-cybersecurity-defector-warns-of-North-Korea-s-hacker-army.

363 Steve Miller, "Where Did North Korea's Cyber Army Come From?" Voice of America, November 20, 2018, https://www.voanews.com/east-asia-pacific/where-did-north-koreas-cyber-army-come.

364 Ju-min Park, "Exclusive: North Korea's Unit 180, the Cyber Warfare Cell That Worries the West," Reuters, May 22, 2017, https://www.reuters.com/article/us-cyber-northkorea-exclusive/exclusive-north-koreas-unit-180-the-cyber-warfare-cell-that-worries-the-west-idUSKCN18H020.

365 "North Korea 'Stole $2bn for Weapons via Cyber-Attacks'," BBC News, August 7, 2019, https://www.bbc.com/news/world-asia-49259302.

366 "Treasury Sanctions North Korean State=Sponsored Malicious Cyber Groups," Department of the Treasury, press release, September 13, 2019, https://home.treasury.gov/news/press-releases/sm774.

367 Elizabeth Shim, "North Korean Hackers Suspected in India Space Agency Cyberattack," UPI, November 7, 2019, https://www.upi.com/Top_News/World-News/2019/11/07/North-Korean-hackers-suspected-in-India-space-agency-cyberattack/7371573053505/.

368 Sean Lyngaas, "Lazarus Rises in Israel with Attempted Hack of Defense Company, Researchers Say," CyberScoop, June 7, 2019, http://www.cyberscoop.com/lazarus-rises-israel-attempted-hack-defense-company-researchers-say/.; and Sherisse Pham, "Here's a new North Korean hacking threat to worry about," CNN Business, February 20, 2018, https://money.cnn.com/2018/02/20/technology/north-korea-hackers-reaper-fireeye/index.html.

INDIA

369 "Orbital Launches of 2019," Gunter's Space Page, February 11, 2020, https://space.skyrocket.de/doc_chr/lau2019.htm.

370 Chethan Kumar, "India to launch first manned space mission by 2022: PM Modi," *Times of India,* August 15, 2018, https://timesofindia.indiatimes.com/india/india-to-launch-first-manned-space-mission-by-2022-pm-modi/articleshow/65410373.cms.

371 Indian Space Research Organization, "Annual Report 2019-2020," Department of Space, 2020, 94, https://www.isro.gov.in/sites/default/

files/flipping_book/annual_report_2019-20_english/files/assets/common/downloads/Annual%20Report%202019-20%20(English).pdf.

372 Note: Data limited to total launches from 1980 to 2019; Thomas G. Roberts, *Spaceports of the World* (Washington, DC: CSIS, March 2019), https://www.csis.org/analysis/spaceports-world.

373 "India launches record 104 satellites in single mission," BBC News, February 15, 2017, https://www.bbc.com/news/world-asia-india-38977803.

374 "Space Environment: Total Payloads Launched by Country," accessed February 12, 2020.

375 Staff Writers, "ISRO's Second Spaceport, for New SSLV Rocket, to Come up in Tamil Nadu," *The Wire*, December 1, 2019, https://thewire.in/space/isro-kulasekarapattinam-thoothukudi-sdsc-sriharikota-sslv-pslv-gslv-antrix.

376 Surendra Singh, "India to get its second spaceport, and acquisition work begins in Tamil Nadu," *Times of India,* December 2, 2019, https://timesofindia.indiatimes.com/india/india-to-get-its-second-spaceport-land-acquisition-work-begins-in-tamil-nadu/articleshow/72323869.cms.

377 Jeff Foust, "Spaceflight purchases first commercial flight of new Indian small launcher," SpaceNews*,* August 6, 2019, https://spacenews.com/spaceflight-purchases-first-commercial-flight-of-new-indian-small-launcher/.

378 Connor Simpson, "China Becomes Third Country to Ever 'Soft-Land' on the Moon," *The Atlantic*, December 14, 2013, https://www.theatlantic.com/international/archive/2013/12/china-becomes-third-country-ever-soft-land-moon/356151/.

379 Elizabeth Howell, "Chandrayaan-2: India's Orbiter-Lander-Rover Mission," Space.com, October 8, 2019, https://www.space.com/40136-chandrayaan-2.html.

380 Ibid.

381 Chelsea Gohd, "India Admits Its Moon Lander Crashed, Cites Problem with Breaking Thrusters," Space.com, November 25, 2019, https://www.space.com/india-admits-moon-lander-crash.html.

382 Jeff Foust, "India confirms plans for a second lunar lander mission," SpaceNews, January 1, 2020, https://spacenews.com/india-confirms-plans-for-second-lunar-lander-mission/.

383 Staff Writers, "Indian astronauts to begin training in Russia for country's first manned space mission," SpaceDaily, January 23, 2020, http://www.spacedaily.com/reports/Indian_astronauts_to_begin_training_in_Russia_for_countrys_first_manned_space_mission_999.html.

384 Ibid.

385 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/?utm_medium=social&utm_source=twitter.com&utm_campaign=Socialflow+DFN.

386 Rajat Pandit, "India to hold first simulated space warfare exercise next month," *Times of India*, June 8, 2019, https://timesofindia.indiatimes.com/india/india-to-hold-first-simulated-space-warfare-exercise-next-month/articleshow/69697289.cms.

387 Raghuvanshi, "India to launch a defense-based space research agency."

388 Pandit, "India to hold first simulated space warfare exercise next month."

389 Ajay Banerjee, "India plans policy to tackle space threats," *Tribune*, July 29, 2019, https://www.tribuneindia.com/news/archive/india-plans-policy-to-tackle-space-threats-809330.

390 Indian Space Research Organization, "Annual Report 2019-2020," 94.

391 Ashley J. Tellis, "India's ASAT Test: An Incomplete Success," Carnegie Endowment for International Peace, April 15, 2019, https://carnegieendowment.org/2019/04/15/india-s-asat-test-incomplete-success-pub-78884.

392 Ibid.

393 Jonathan McDowell, Twitter Post, December 27, 2019, 8:54 PM, https://twitter.com/planet4589/status/1210786046943739904.

394 Sarah Lewin, "India's Anti-Satellite Test Created Dangerous Debris, NASA Chief Says," Space.com, April 1, 2019, https://www.space.com/nasa-chief-condemns-india-anti-satellite-test.html.

395 Chitranjan Kumar, "India tests ASAT: China calls for peace, Pakistan urges international community to condemn," *Business Today*, March 27, 2019, https://www.businesstoday.in/current/economy-politics/india-tests-asat-china-calls-for-peace-pakistan-urges-international-community-to-condemn/story/331703.html.

396 Doris Elin Urrutia, "India's Anti-Satellite Missile Test Is a Big Deal. Here's Why.," Space.com, March 30, 2019, https://www.space.com/india-anti-satellite-test-significance.html.

397 Tellis, "India's ASAT Test."

398 Shaan Shaikh, "India Conducts Successful ASAT Test," Missile Threat, CSIS, March 28, 2019, https://missilethreat.csis.org/india-conducts-successful-asat-test/.

399 Narendra Modi, Twitter Post, March 27, 2019, 12:08 AM, https://twitter.com/narendramodi/status/1110800868058660864.

400 Ibid.

401 Rajat Pandit, "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.

402 Pearl MAria D'Souza, "French Agency CNES to aid ISRO's space station project," *New Indian Express*, January 27, 2020, https://www.newindianexpress.com/nation/2020/jan/27/french-agency-cnes-to-aid-isros-space-station-project-2094922.html.

403 Snehesh Alex Philip, "India gets new Special Ops Division that can cripple targets miles inside enemy territory," ThePrint, May 15, 2019, https://theprint.in/defence/india-gets-new-special-ops-division-that-can-cripple-targets-miles-inside-enemy-territory/235786/.

404 Amrita Nayak Dutta, "New tri services special ops division, meant for surgical strikes, finishes 1st exercise today," ThePrint, September 28, 2019, https://theprint.in/defence/new-tri-services-special-ops-division-meant-for-surgical-strikes-finishes-1st-exercise-today/298445/.

405 Rajat Pandit, "After Agni-V Launch, DRDO's New Target Is Anti-satellite Weapons," *Times of India*, April 20, 2012, https://timesofindia.indiatimes.com/india/After-Agni-V-launch-DRDOs-new-target-is-anti-satellite-weapons/articleshow/12763074.cms.

406 Headquarters Integrated Defence Staff, *Technology Perspective and Capability Roadmap (TPCR)* (New Delhi: India Ministry of Defence, April 2013), 6-7, 32-33, https://mod.gov.in/sites/default/files/TPCR13.pdf.

407 Headquarters Integrated Defence Staff, *Technology Perspective and Capability Roadmap (TPCR)* - 2018 (New Delhi: India Ministry of Defence, 2018), 21-22, https://mod.gov.in/sites/default/files/tpcr.pdf.

408 Rajat Pandit, "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.

409 Brian Weeden and Victoria Samson, "India's ASAT test is a wake-up call for norms of behavior in space," *SpaceNews*, April 8, 2019, https://spacenews.com/op-ed-indias-asat-test-is-wake-up-call-for-norms-of-behavior-in-space/.

410 Daniel Oberhaus, "India's Anti-Satellite Test Wasn't Really About Satellites," *Wired*, March 27, 2019, https://www.wired.com/story/india-anti-satellite-test-space-debris/.

411 Headquarters Integrated Defence Staff, *Technology Perspective and Capability Roadmap (TPCR) - 2018*, 63.

412 Ibid., 64.

413 PTI, "Govt approves setting up of defence cyber agency," *Times of India*, November 27, 2019, https://timesofindia.indiatimes.com/india/govt-approves-setting-up-of-defence-cyber-agency/articleshow/72264836.cms.

414 Ibid.

415 "Orbital Launches of 2019," Gunter's Space Page, February 11, 2020, https://space.skyrocket.de/doc_chr/lau2019.htm

416 John Raymond and Kathleen Hicks, "A Conversation with General Raymond" (public event, Center for Strategic and International Studies, Washington, D.C.: November 2019) 18, https://www.csis.org/analysis/conversation-general-raymond.

417 Louis de Gouyon Matignon, "The Birth of the French Space Program," Space Legal Issues, February 2, 2019, https://www.spacelegalissues.com/space-law-the-birth-of-the-french-space-program/.

418 "Insight," CNES, November 27, 2018, https://insight.cnes.fr/en/INSIGHT/index.htm.

419 "World First French SEIS Instrument Detects 'Marsquake'," CNES, April 23, 2019, https://presse.cnes.fr/en/world-first-french-seis-instrument-detects-marsquake.

420 Kyle Mizokami, "France Accuses Russia of Space Satellite Espionage," *Popular Mechanics*, September 10, 2018, https://www.popularmechanics.com/military/a23067892/france-charges-russia-with-space-satellite-espionage/.

421 Space Environment: Total Payloads Launched by Country," accessed February 12, 2020.

422 "Defense Space Strategy Summary," French Ministry of Defense, DICoD Publishing Office, July 2019, https://www.defense.gouv.fr/content/download/563617/9727377/synthe%CC%80se%20strate%CC%81gie%20spatiale%20de%20de%CC%81fense.pdf.

423 Theresa Hitchens, "Space Lasers for Satellite Defense Top New French Space Strategy," Breaking Defense, July 26, 2019, https://breakingdefense.com/2019/07/france-envisions-on-orbit-lasers-for-satellite-defense/.

424 Florence Parly, "Presentation of the Defense Space Strategy," SatelliteObservation.net, July 25, 2019, English translation from: https://satelliteobservation.net/2019/07/27/frances-new-space-defense-strategy/.

425 Hitchens, "Space Lasers for Satellite Defense Top New French Space Strategy."

426 Jen Judson, "US, Israel's Arrow-3 missile put to the test in Alaska," *Defense News*, July 28, 2019, https://www.defensenews.com/pentagon/2019/07/28/us-israels-arrow-3-missile-put-to-the-test-in-alaska/.

427 Ibid.

428 "Tesla Model 3 Spoofed off the highway - Regulus Navigation System Hack Causes Car to Turn On Its Own," Regulus, n.d., https://www.regulus.com/blog/tesla-model-3-spoofed-off-the-highway-regulus-researches-hack-navigation-system-causing-car-to-steer-off-road/.

429 Ibid.

430 Josh Petri, "How Hackers Can Take Over Your Car's GPS," Hyperdrive, June 19, 2019, https://www.bloomberg.com/news/articles/2019-06-19/threat-of-gps-spoofing-for-autonomous-cars-seen-as-overblown.

431 Ibid.

432 "Arrow 3 (Israel)," Missile Threat, CSIS, August 11, 2016, last modified June 15, 2018, https://missilethreat.csis.org/defsys/arrow-3/.

433 "2020: The Year of Sustainability," *AviationWeek & Space Technology,* January 2020, 17, https://aviationweek.com/sites/default/files/2020-01/AW_200113_0.pdf.

OTHERS

434 Mari Yamaguchi, "Japan reveals plan for space defense unit," *Defense News*, January 21, 2020, https://www.defensenews.com/space/2020/01/21/japan-reveals-plan-for-space-defense-unit/.

435 Mari Yamaguchi, "Abe says new unit will defend Japan from space tech threats," MSN, January 20, 2020, https://www.msn.com/en-us/news/world/abe-says-new-unit-will-defend-japan-from-space-tech-threats/ar-BBZ8kfk#image=BBZ8kfk_1|2.

436 Yamaguchi, "Japan reveals plan for space defense unit."

437 Yomiuri Shimbum, "Satellite interceptor sought by mid-2020s," *Japan News*, August 19, 2019, https://the-japan-news.com/news/article/0005948349.

438 Ibid.

439 Ibid.

440 Euan McKirdy, "Hayabusa mission: Japanese space probe attempts to 'bomb' asteroid," CNN, April 5, 2019, https://www.cnn.com/2019/04/05/asia/hayabusa-crater-operation-sci-intl/index.html.

441 Allied Maritime Command, "Electronic Interference in Mediterranean," December 12, 2019, https://shipping.nato.int/nsc/operations/news/2019/electronic-interference-in-mediterranean.

442 Ibid.

443 Alexandra Sticklings, "UK Ministry of Defence Announces Ambitious Plans for Space," Royal United Services Institute, July 30, 2019, https://rusi.org/commentary/uk-ministry-defence-announces-ambitious-plans-space.

444 Sandra Erwin, "As satellites become targets, UK military seeks closer ties with space industry," SpaceNews, November 6, 2018, https://spacenews.com/as-satellites-become-targets-u-k-military-seeks-closer-ties-with-space-industry/.

445 Andrew Chuter, "UK shoots for new laser weapons against drones, missiles," *Defense News*, July 9, 2019, https://www.defensenews.com/global/europe/2019/07/09/uk-shoots-for-new-laser-weapons-against-drones-missiles/.

446 Mandy Zuo, "China flight systems jammed by pig farm's African swine fever defences," *South China Morning Post*, December 20, 2019, https://www.scmp.com/news/china/society/article/3042991/china-flight-systems-jammed-pig-farms-african-swine-fever.

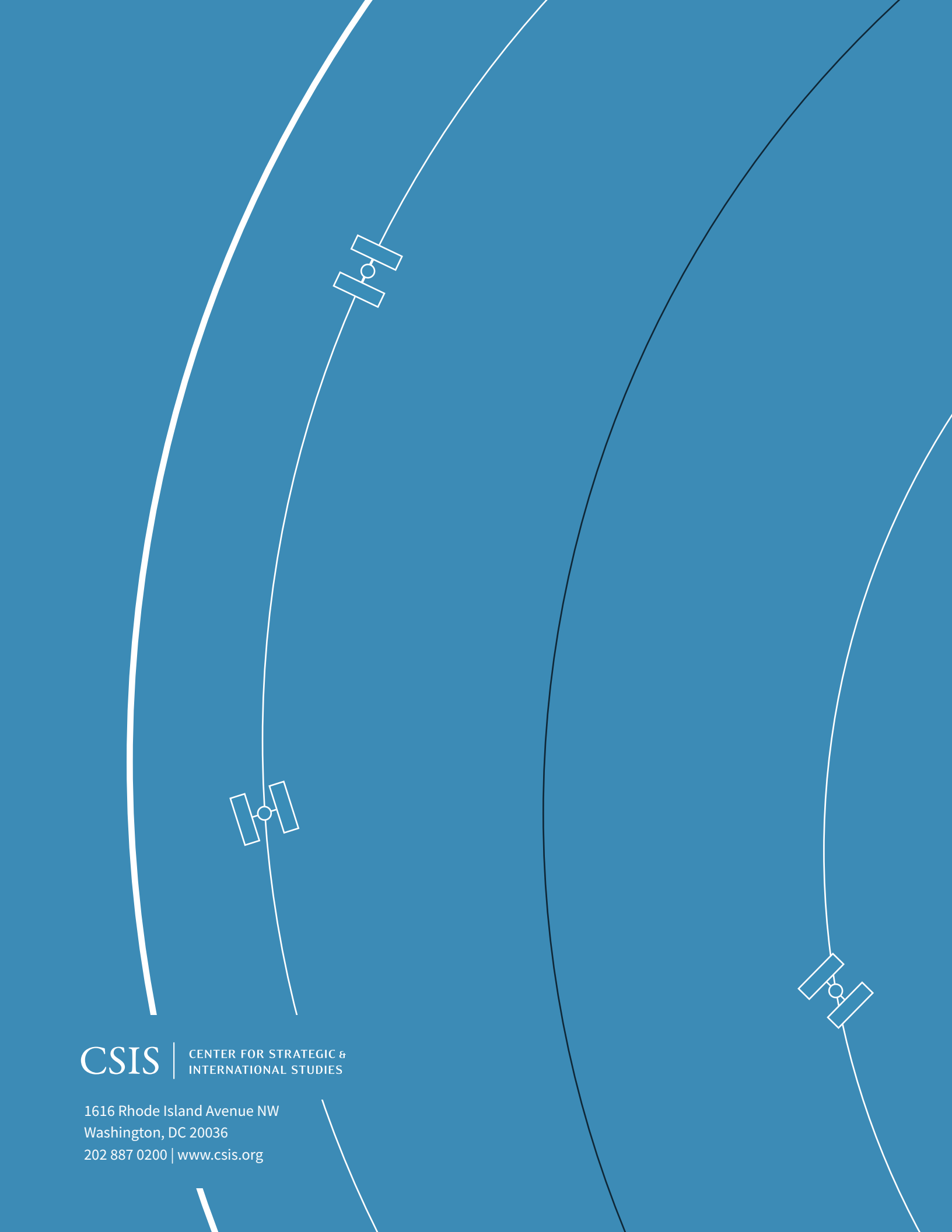
447 Editor, "GPS Signal Jamming Destroys China Drone Show - Again," Resilient Navigation and Timing Foundation, November 1, 2018, https://rntfnd.org/2018/11/01/gps-jamming-destroys-china-drone-show-again/.

448 Simone McCarthy, William Zheng, and Denise Tsang, "HK$1 million in damage caused by GPS jamming that caused 46 drones to plummet during Hong Kong show," *South China Morning Post*, October 29, 2018, https://www.scmp.com/news/hong-kong/law-and-crime/article/2170669/hk13-million-damage-caused-gps-jamming-caused-46-drones.

449 Katherine Dunn, "The long ocean voyage that helped find the flaws in GPS," *Fortune*, January 24, 2020, https://fortune.com/2020/01/24/gps-disruption-test-voyage/.

450 Ibid.

451 Ibid.



CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

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