APRIL 2019

A REPORT OF THE CSIS AEROSPACE SECURITY PROJECT

SPACE THREAT ASSESSMENT 2019

Principal Authors
TODD HARRISON
KAITLYN JOHNSON
THOMAS G. ROBERTS

Contributing Authors
MADISON BERGETHON
ALEXANDRA COULTRUP

Foreword
REP. JIM COOPER (D-TN)

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

APRIL 2019

SPACE THREAT ASSESSMENT 2019

Principal Authors
TODD HARRISON
KAITLYN JOHNSON
THOMAS G. ROBERTS

Contributing Authors
MADISON BERGETHON
ALEXANDRA COULTRUP

Foreword
REP. JIM COOPER (D-TN)

A REPORT OF THE
CSIS AEROSPACE SECURITY PROJECT

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES | AEROSPACE SECURITY PROJECT

ABOUT CSIS

Established in Washington, D.C., over 50 years ago, the Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to providing strategic insights and policy solutions to help decisionmakers chart a course toward a better world.

In late 2015, Thomas J. Pritzker was named chairman of the CSIS Board of Trustees. Mr. Pritzker succeeded former U.S. senator Sam Nunn (D-GA), who chaired the CSIS Board of Trustees from 1999 to 2015. CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

Founded in 1962 by David M. Abshire and Admiral Arleigh Burke, CSIS is one of the world's preeminent international policy institutions focused on defense and security; regional study; and transnational challenges ranging from energy and trade to global development and economic integration. For eight consecutive years, CSIS has been named the world's number one think tank for defense and national security by the University of Pennsylvania's "Go To Think Tank Index."

The Center's over 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look to the future and anticipate change. CSIS is regularly called upon by Congress, the executive branch, the media, and others to explain the day's events and offer bipartisan recommendations to improve U.S. strategy.

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 Rep. Jim Cooper (D-TN), Brian Weeden, Matthew P. Funaiole, and Caroline Amenabar for their support of this project.

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 2003
202-887-0200 | www.csis.org

CONTENTS

FOREWORD

WE ARE ALMOST AS DEPENDENT ON SATELLITES as we are on the sun itself. They are our "infrastructure of infrastructure," enabling our television, internet, telecommunications, energy, trade, and financial networks to function. Who wouldn't be lost without GPS, the free service we have given the world?

Satellites already crowd key orbits. And companies like SpaceX and Blue Origin are building cheaper, reusable rockets to add as many as 100 new satellites with every launch.

Every nation's satellites face increasing threats, starting with killer debris in the vast supersonic junkyards circling the earth. Even a paint chip is lethal at 17,000 miles per hour. Fortunately, the U.S. Air Force tracks the larger threats and warns all spacefaring nations how to maneuver their satellites to safety. We provide free space traffic control to every nation.

Satellites are also vulnerable to a wide array of intentional threats, such as killer satellites. Other nations have learned how to attack the global commons of space. Our vulnerability is acute because our satellites are the juiciest targets. Cripple our satellites, and you cripple us. Satellites are not only our crown jewels but the crown itself—and we have no castle to protect them.

The United States is not the leader in anti-satellite technology. We had naively hoped that our satellites were simply out of reach, too high to be attacked, or that other nations would not dare. As this report meticulously documents, other nations are developing, testing, and fielding a range of counterspace weapons that threaten to deprive us of the many economic and military advantages we derive from space.

The risk of a space Pearl Harbor is growing every day. Yet this war would not last for years. Rather, it would be over the day it started. Without our satellites, we would have a hard time regrouping and fighting back. We may not even know who had attacked us, only that we were deaf, dumb, blind, and impotent.

We have been officially warned of this danger since at least 2001 when the Rumsfeld Report was released, but the Pentagon has done very little to reduce this existential risk. The 2008 Allard Report even warned that "no one is in charge" of our space strategy. Sadly, this is still true.

This is the year of decision. The House of Representatives has overwhelmingly and on a bipartisan basis supported a new "Space Corps" for several years, and the president has recently demanded a "Space Force." The Pentagon has responded with a proposal that assembles a Space Force that resembles the House's Space Corps proposal. This year's National Defense Authorization Act will decide the outcome. ○

REP. JIM COOPER (D-TN)

United States House of Representatives

INTRODUCTION

OVER THE PAST YEAR, much of the focus on national security space issues has revolved around proposals to reorganize the national security space enterprise by creating an independent military service for space, re-establishing United States Space Command as the combatant command for space, and standing up a Space Development Agency for innovative space technologies and programs. While each of these proposals has generated some controversy and skepticism, the energy and attention they have garnered reflects a broader recognition of the important role space systems play in overall U.S. national security.

The United States is increasingly dependent on space both economically and militarily. From the Global Positioning System (GPS) timing signals on which many industries rely to the missile warning systems that underpin U.S. nuclear deterrence, the United States and its allies and partners around the world depend on space for security and prosperity. U.S. military strategy relies on being able to project power around the world and over great distances—something space-based capabilities are uniquely able to support. But as the United States has developed more advanced national security space systems and integrated them into military operations in increasingly sophisticated ways, space systems have become a more attractive target for adversaries to exploit.

"New threats to commercial and military uses of space are emerging, while increasing digital connectivity of all aspects of life, business, government, and military creates significant vulnerabilities. During conflict, attacks against our critical defense, government, and economic infrastructure must be anticipated."

2018 NATIONAL DEFENSE STRATEGY, UNITED STATES DEPARTMENT OF DEFENSE[1]

A common theme heard among the national security policy community is that space has now become a contested warfighting domain. But this is not true—space has been a contested warfighting domain from the beginning. The first anti-satellite (ASAT) weapon was tested by the United States in 1959, just two years after the launch of Sputnik, and both the Soviet Union and the United States continued developing and testing anti-satellite weapons of various kinds throughout the Cold War.[2] What is different now is that our ability to deter attacks against space systems has become less certain, and a wide range of counterspace weapons are proliferating to hostile nations and non-state actors.

While the vulnerabilities of U.S. national security space systems are often discussed publicly, the progress other nations are making in counterspace systems is not as readily accessible. The purpose of this report is to review the open-source information available on the counterspace capabilities that can threaten U.S. space systems. 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 their attention. The report focuses on four specific countries that pose the greatest risk for the United States: China, Russia, Iran, and North Korea. A fifth section analyzes the counterspace capabilities of select other countries, including some allies and partners of the United States, and some non-state actors.

This report is not a comprehensive assessment of all known threats to U.S. space systems because much of the information on what other countries are doing to advance their counterspace systems is not publicly available. Instead, it serves as an unclassified assessment that aggregates and highlights open-source information on counterspace capabilities for policymakers and the general public. The information in this report is current as of February 22, 2019.

TYPES OF COUNTERSPACE WEAPONS

"Our adversaries have been working to bring new weapons of war into space itself ... As their actions make clear, our adversaries have transformed space into a warfighting domain already."

VICE PRESIDENT MIKE PENCE[3]

IN AUGUST 2018, Vice President Mike Pence laid out the Trump administration's plans for space reorganization in a speech delivered at the Pentagon. In his remarks, the Vice President spoke at length about the threats posed to U.S. space systems by other nations, specifically Russia and China.

> *"Russia has been designing an airborne laser to disrupt our space-based system[s]. And it claims to be developing missiles that can be launched from an aircraft mid-flight to destroy American satellites. Both China and Russia have been conducting highly sophisticated on-orbit activities that could enable them to maneuver their satellites into close proximity of ours, posing unprecedented new dangers to our space systems."*[4]

Counterspace weapons are not just limited to the handful of examples cited by the vice president. A wide array of counterspace weapons are available to potential adversaries that vary in the types of effects they create, the level of technological sophistication, and the resources required to develop and field them. Counterspace weapons also differ in how they are employed and how difficult they are to detect and attribute. The effects of these weapons can also be temporary or permanent, depending on the type of system and how it is used. This assessment uses four broad categories to discuss different types of counterspace weapons: kinetic physical, non-kinetic physical, electronic, and cyber.

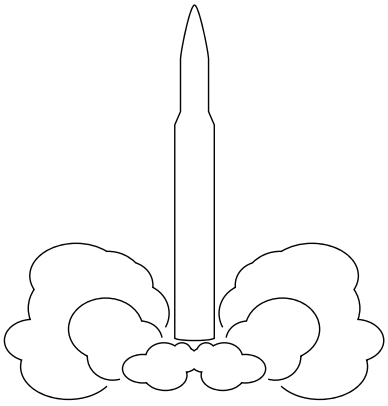
KINETIC PHYSICAL

KINETIC PHYSICAL COUNTERSPACE weapons attempt to strike directly or detonate a warhead near a satellite or ground station. 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 and then, when commanded, maneuvers to strike its target. Co-orbital ASATs can remain dormant in orbit for days or even years before being activated.[5]

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 on-board guidance system requires a relatively high level of technological sophistication and significant resources to test and deploy. A co-orbital ASAT without an on-board guidance system, such as a satellite that is repurposed to intentionally maneuver into the path of another satellite, can be a nuisance and interfere with the normal operation of the targeted satellite by forcing it to maneuver to safety. However, an incident like this is unlikely to pose a serious collision risk without the advanced guidance and targeting capabilities needed to make it an effective weapon.

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.

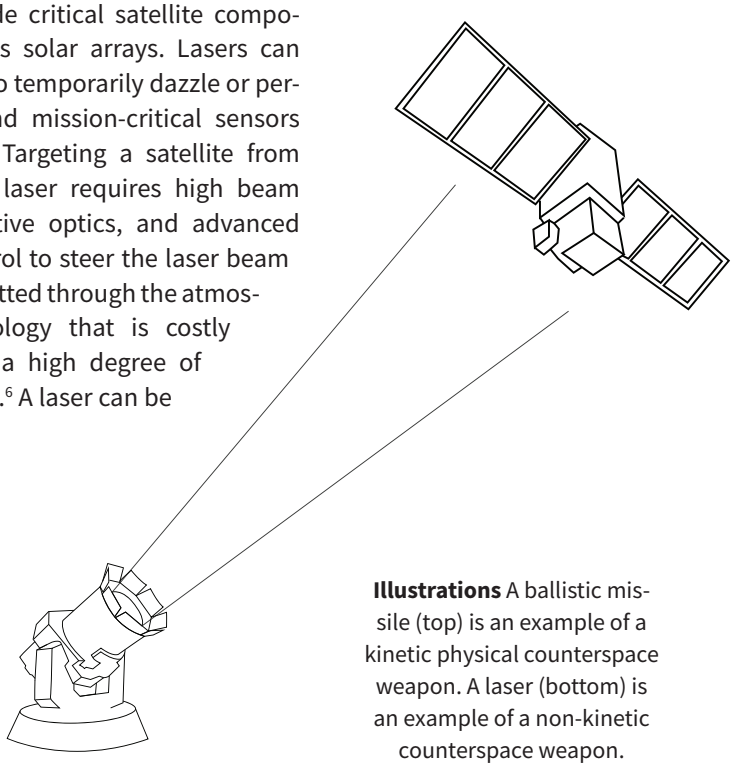
Kinetic physical attacks have catastrophic and irreversible effects on the satellites and ground stations targeted. These counterspace weapons are likely to be attributable because the United States and others can identify the source of a direct-ascent ASAT launch or ground attack, and can, in theory, 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, such as orbital debris or a damaged ground station.



NON-KINETIC PHYSICAL

NON-KINETIC COUNTERSPACE weapons, such as lasers, high-powered microwaves (HPM), 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 critical 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.[6] A laser can be



Illustrations A ballistic missile (top) is an example of a kinetic physical counterspace weapon. A laser (bottom) is an example of a non-kinetic counterspace weapon.

effective against a sensor on a satellite if it is within the field of view of its sensors, 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 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 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 back-door HPM attack attempts to enter through small seams or gaps around electrical connections and shielding.[7] 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 or a high-flying airborne platform. 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 is an indiscriminate form of non-kinetic physical attack. While a nuclear detonation would have immediate effects for satellites within range of the electromagnetic pulse it creates, it also creates a high radiation environment that accelerates the degradation of satellite components over the long-term for all unshielded satellites in the affected orbital regime.[8]

ELECTRONIC

ELECTRONIC ATTACKS TARGET the means by 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. Jamming is a reversible form of attack because once a jammer is turned off, communications return to normal.

Commercial and military satellites are susceptible to both uplink and downlink jamming.[9] The uplink is the signal going from a ground station or user terminal to the satellite, while the downlink is the signal that is sent from the satellite back to a ground station or user terminal.[10] An uplink jammer interferes with the signal going to a satellite, such as the command and control uplink, if it is within the field of view of the antenna on the receiving satellite.[11] Downlink jammers target the satellite's users by creating noise in the same frequency and at roughly the same power as the downlink signal within the field of view of the receiving terminal's antenna.[12] User terminals with omnidirectional antennas, such as many GPS receivers and satellite phones, have a wider field of view and thus are more susceptible to downlink jamming from different angles on the ground.

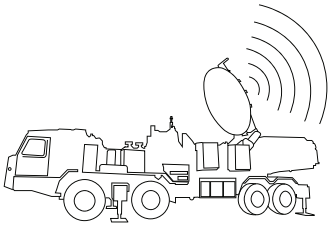


Illustration A truck-mounted GPS jammer is a type of electronic counterspace weapon.

Spoofing Yachts in the Mediterranean Sea

IN THE SUMMER OF 2013, a group of students from The University of Texas at Austin successfully demonstrated the ability to spoof a GPS signal, causing a private yacht to veer off of its GPS-guided course in the Mediterranean Sea.[15] Using a small spoofing device—approximately the size of a briefcase—the student researchers redirected the ship hundreds of meters away from its intended trajectory without being detected.

While GPS jamming makes it difficult for a receiver to determine its own location, often raising an alarm message to the user, a spoofing attack is more devious. GPS spoofing can fool a receiver into calculating an incorrect position, potentially subverting loss-of-signal alarms in the process.

The technology needed to jam many types of satellite signals is commercially available and relatively inexpensive. 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.[13]

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

Through a type of spoofing called 'meaconing,' even encrypted military GPS signals can be spoofed. Meaconing does not require cracking the GPS encryption because it merely rebroadcasts a time-delayed copy of the original signal without decrypting it or altering the data.[14] 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 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. These different types of cyberattacks vary in terms of the difficulty and technical sophistication required. 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 can potentially pose a cyber threat.[16]

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.

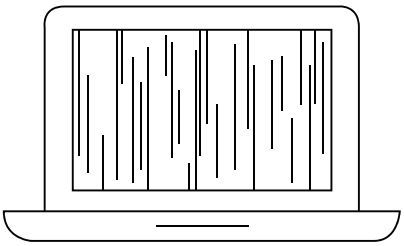


Illustration
Data monitoring is a type of cyber counterspace weapon.

THREAT CHARACTERISTICS

THE TYPES OF COUNTERSPACE THREATS described above have distinctly different characteristics that make them more or less suitable for different situations. As shown in Table 1, some types of threats are difficult to attribute or have fully reversible effects, such as mobile, intermittent 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 or create uncertainty in the mind of its opponent 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 unintentionally and turning other nations against the attacker other nations against the attacker, or could damage the attacker's own space systems.

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	Unsystematic effects from higher radiation lelvels 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	Only satellite operator will be aware	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 2018[17]
38

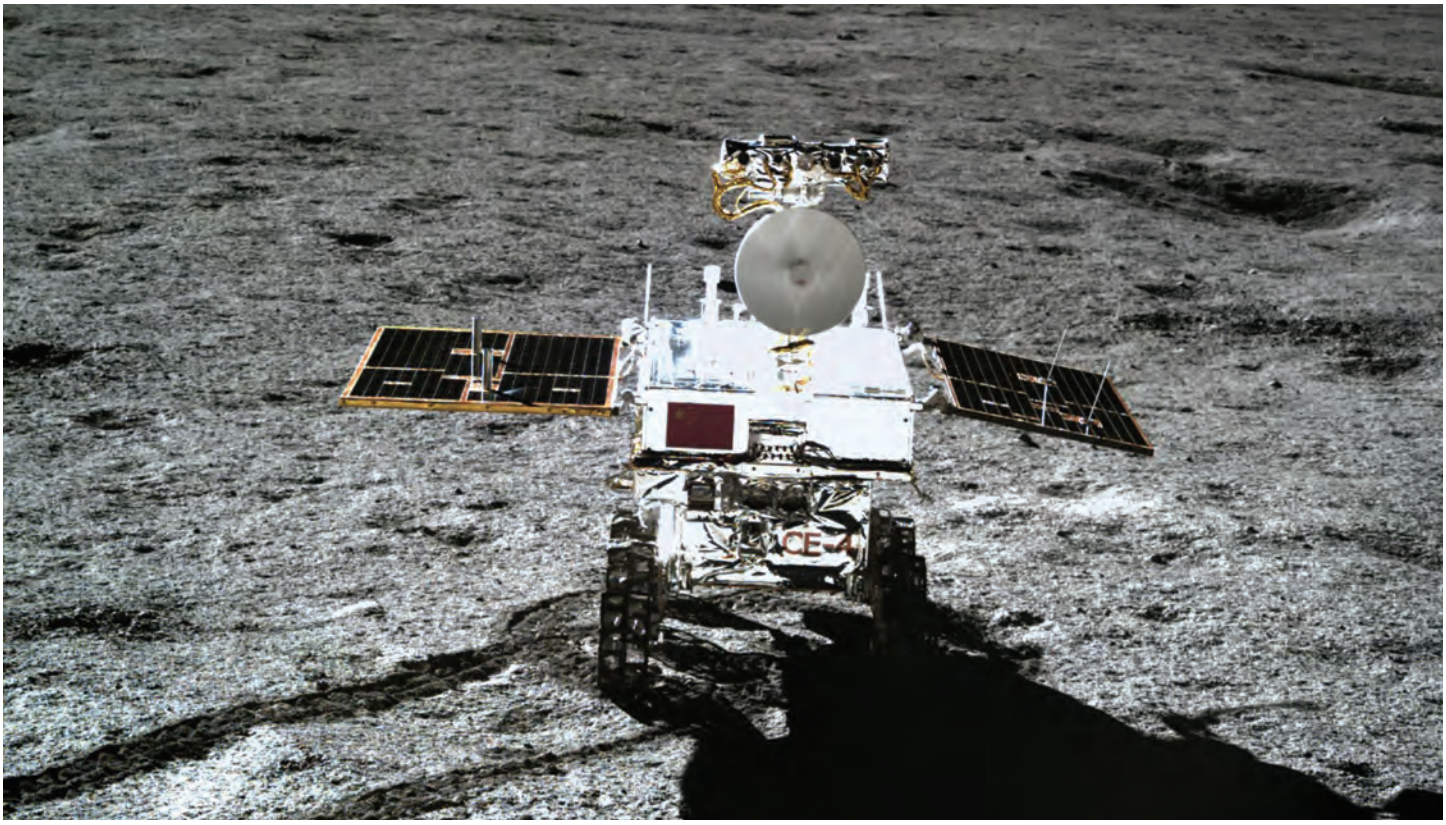
CHINA

"Exploring the vast universe, developing space programs and becoming an aero-space power have always been the dream we've been striving for."

PRESIDENT XI JINPING[18]

SINCE ITS FIRST SATELLITE LAUNCH in April 1970, China has been steadily progressing as a global space power. A string of Chinese space achievements has marked the past 20 years including launching a human into orbit, successfully operating two space stations, and most recently, landing a lunar rover on the far side of the Moon. Carried into orbit by its robust family of Long March space launch vehicles, China is progressing rapidly in space. In 2018, China conducted 38 orbital launches, surpassing the United States' 34 launches.[19] China plans to attempt over 30 launches in 2019, including 10 satellites for positioning, navigation, and timing (PNT), as well as a new launch capability, the Long March 11 via a sea-based platform.[20] The Long March 5—the country's heavy lift launch system—will return to operation after a two-year hiatus in July 2019. If all goes well, the Long March 5 will launch China's next lunar probe and return lunar samples to Earth at the end of 2019.[21]

China showcased its fast-paced technological advancements and dedication to being a space power this year with its lunar lander *Chang'e*-4. Named after the Chinese goddess of the Moon, the *Chang'e* spacecraft successfully landed on the far side of the Moon on January 3, 2019, becoming the first ever spacecraft to do so. The lunar rover, *Yutu*-2, is named after the goddess *Chang'e*'s pet rabbit. Thus far, the mission has already been a great success, reporting that the surface temperature on the far side of the moon drops to well below -300 degrees Fahrenheit. The rover will continue its science and exploration missions in the upcoming months.[23] These advancements showcase China's civil space aspirations.



Yutu-2 became the first lunar rover to explore the far side of the Moon in January 2019. The rover is part of the Chinese *Chang'e*-4 mission, which launched on December 7, 2018.

AFP / GETTY IMAGES

China is also moving forward with a new modular space station. China has successfully operated two previous space labs in Low Earth Orbit (LEO), *Tiangong*-1 and -2 through its Project 921 program, which began in 1992.[24] The new space station will consist of three modules. The core module for the new space station is expected to be launched in 2020, while the two additional experimental modules are planned for launch in 2021 and 2022. Three or four manned missions, and several cargo missions, are also planned for 2021–2022.[25] The station is estimated to have a 10 year lifespan, with the possibility of an extension.[26] China is also currently developing a new space telescope, called *Xuntian*—meaning "Heavenly Cruiser" in Mandarin—which will reportedly have a field of view 300 times larger than the U.S. Hubble Space Telescope. This telescope will be placed near the new space station in the case that astronauts need to service it manually.[27]

In 2017, it was estimated that China spent almost $11 billion on space, across its civil and military programs. This was the second most spending for any country on space activities in 2017, behind the United States.[28] Information on China's 2018 civil and military space spending is not yet publicly available.

As China continues to invest more in its own state-run space programs, it is also becoming one of the largest investors in private companies. As a recent Department of Defense (DoD) report to Congress

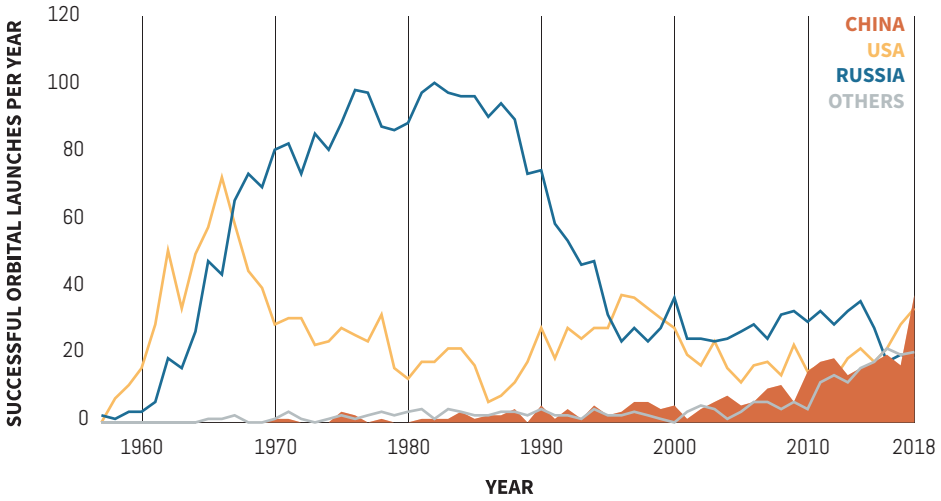


Figure 1: Chinese orbital space launches (1957–2018). China supported more successful orbital space launches in 2018 than it did in the entire first space age, from 1957 to 1991.

SPACE-TRACK.ORG / CSIS AEROSPACE SECURITY[22]

noted, Chinese president Xi Jinping "has emphasized the importance of science and technology (S&T) innovation, both for rejuvenating China and modernizing China's military." Commercial advances in science and technology are often incorporated into China's military capabilities.[29] The Chinese government invested approximately $336 million in private Chinese space companies in 2018.[30] One of the most active China-based private investors, Tencent Holdings, has also invested in several U.S.-based space start-ups such as Moon Express, Planetary Resources, and World View Enterprises.[31]

After a 2014 decree to allow private companies to develop space launch vehicles, several new nominally private, but often state-backed, Chinese companies began to develop and test new launch vehicles. In 2017, the government made a $182 million investment in a new launch company called ExPace Technology, which to-date is still "the largest investment in a non-U.S. space start-up."[32] Similarly, One Space, another Chinese launch company, received $44 million in Series B funding in 2018 after successfully launching its first and second sub-orbital payloads in May and September, respectively, earlier that year.[33] One Space is looking to launch its first orbital payload in the first half of 2019. Another company called iSpace—also known as Beijing Interstellar Glory Space Technology Ltd.—completed a sub-orbital launch of its single-stage rocket known as Hyperbola-1Z in mid-2018 and plans to launch three more times in 2019.[34]

In October 2018, the first Chinese commercial orbital launch was attempted by a new company called LandSpace. A third-stage malfunction prevented the rocket, called *Zhuque* 1, from reaching orbit. The company intends to build two larger rockets and provide heavier lift capabilities to LEO.[35]

To further improve its space capabilities, China is continuing to rapidly develop and launch both intelligence, surveillance, and reconnaissance (ISR) satellites and PNT satellites. This PNT system, called the *Beidou* satellite system, gives China independence from the United States' GPS constellation for military and commercial applications. China has also been providing access to the *Beidou* system to its partners and allies as coverage grows. By 2020, China "plans to establish a global, 24-hour, all-weather earth remote sensing system and a global satellite navigation system."[36]

AS CHINA CONTINUES TO INVEST MORE IN ITS OWN STATE-RUN SPACE PROGRAMS, IT IS ALSO BECOMING ONE OF THE LARGEST INVESTORS IN PRIVATE COMPANIES.

Furthermore, to increase its ISR capabilities, in July 2018 China launched its highest resolution imagery satellite to-date, *Gaofen*-11, part of the China High-resolution Earth Observation System (CHEOS). CHEOS is intended to provide meteorological coverage through "advanced optical and synthetic aperture radar satellites, and could also include airborne and near-space systems such as stratospheric balloons." It is expected to be completed by 2020.[37] China has also experimented with new capabilities in space, including such feats as launching the first-ever quantum communications satellite in 2016.[38]

SPACE ORGANIZATION AND DOCTRINE

CHINA'S CIVIL AND MILITARY SPACE activities are run by separate governmental organizations. The State Council's State Administration for Science, Technology, and Industry for National Defense (SASTIND) is the primary organizational force for China's civil space activities. Within SASTIND, the China National Space Administration (CNSA) leads the majority of civil space activities. The China Aerospace Science and Technology Corporation (CASC), a state-owned aerospace corporation, also handles China's burgeoning space program, including developing space launch vehicles, satellites, and related items. Military space activities are run through the People's Liberation Army (PLA). These en-

tities collaborate with one another on developing space technologies.[39]

In 2015, a Chinese white paper stated that "outer space and cyberspace have become new commanding heights in strategic competition among all parties."[40] Many scholars believe that this statement is a formal designation of both space and cyberspace as new warfighting domains.[41] That same year, the PLA founded the Strategic Support Force (SSF) to centralize and manage the military's space, cyber, and electronic warfare missions. The SSF, however, may not have full control over China's anti-satellite (ASAT) capabilities. Specifically, experts believe 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.[42]

Before the 2015 reorganization, responsibilities for cyber, space, and electronic warfare were scattered across at least four different PLA departments. Establishing the SSF indicates the PLA's prioritization of these critical areas of warfare. The PLA leadership publicly recognizes China's growing reliance on space for its expanding military capabilities and reach.[43]

Although many details about the SSF remain unknown, a military parade celebrating the PLA's 90th anniversary in July 2017 featured a formation of electronic reconnaissance officers from the SSF. This group "reportedly provides highly mobile, integrated, flexible, multidomain information warfare capabilities."[44] Featuring the group in the parade indicates the PLA's increasing prioritization of the SSF and its capabilities.[45] The United States Defense Intelligence Agency (DIA) assesses that "strategists in the PLA regard the ability to use space-based systems and deny them to adversaries as central to enabling modern informatized warfare."[46] According to Chinese sources, achieving space superiority means China must ensure its ability to fully utilize its own space assets while simultaneously degrading, disrupting, or destroying its adversary's space capabilities.[47] The PLA is heavily investing in space-based ISR, satellite communications, PNT, and other military space missions.[48] Despite China's many international statements supporting the peaceful use of outer space, the PLA appears to remain focused focused on developing counterspace capabilities.[49]

China views U.S. space and cyber assets as vulnerable. Chinese military scholars wrote in 2007 that "space dominance will be a vital factor in securing air dominance, maritime dominance, and electromagnetic dominance. It will directly affect the course and outcome of wars."[50] In a 2015 report, the U.S.-China Economic and Security Review Commission determined that while China has not published an official, public document detailing its counterspace strategy and doctrine, its actions since the early 2000s indicate that the Chinese program is "primarily designed to deter U.S. strikes against China's space assets, deny space superiority to the United States, and attack U.S. satellites."[51]

COUNTERSPACE WEAPONS

Kinetic Physical

China has proven its kinetic physical counterspace capabilities several times with a range of direct-ascent ASAT systems and conventional mid-course missile interceptors that could potentially be used as an ASAT. Thus far, its primary focus has been targets in LEO. Some experts argue "Chinese [direct-ascent] ASAT capability against deep space targets (Medium Earth Orbit (MEO) and Geosynchronous Orbit (GEO)) is likely still in the experimental or development phase, and there is not sufficient evidence to conclude whether it will become an operational capability in the near future."[53] However, speaking in 2015 then-Lt Gen James Raymond stated at a conference that because of China's investment in ASAT weapons, "soon every satellite in every orbit will be able to be held at risk."[54]

> "China will keep abreast of the dynamics of outer space, deal with security threats and challenges in that domain, and secure its space assets to serve its national economic and social development, and maintain outer space security."
>
> CHINA'S MILITARY STRATEGY, MAY 2015[52]

CHINA

In January 2007, China had its first successful test of a kinetic physical ASAT weapon. This test of a direct-ascent SC-19 missile targeted and destroyed an aging Chinese meteorological satellite, producing hazardous debris in LEO. Over 3,000 trackable pieces of debris have been identified, while thousands of smaller pieces that are unable to be tracked with today's technology continue to pollute LEO. This debris threatens the safe operation of hundreds of other satellites in LEO, including the International Space Station (ISS).[55] China's first two tests of the SC-19 anti-satellite system—occasionally referred to as the DN-1—occurred in 2005 and 2006 from Xichang Satellite Launch Center and were unsuccessful.[56]

As the DIA notes in its assessment, "China has not publicly acknowledged the existence of any new programs since it confirmed it used an ASAT missile to destroy a weather satellite in 2007." Analysts believe several other kinetic physical tests—or suspected tests—have occured since then.[57] In response to the international outrage at China's pollution of LEO, China designed follow-on tests of ASATs to not produce orbital debris.[58] The same SC-19 system was also reportedly tested against ballistic targets in 2010 and 2013 from the Korla Missile Test Complex with success.[59]

U.S. intelligence experts assess that "China probably intends to pursue additional ASAT weapons capable of destroying satellites up to" GEO.[63] A kinetic ASAT attack in GEO could be devastating for the United States and other space-faring nations because the debris it would produce could linger for generations in this unique region of space and interfere with the safe operation of satellites.

Another suspected test was conducted in July 2014. China claimed the launch was a missile interceptor test.[64] Then-assistant secretary of state for arms control verification, and compliance Frank Rose stated that "despite China's claims that this was not an ASAT test, let me assure you the United States has high confidence in its assessment, that the event was indeed an ASAT test."[65] However, experts have noted that "very little information is available in the public record about this launch, other than that it occurred, remained suborbital, and does not appear to have had a clearly evident target, ballistic or otherwise."[66]

China is also suspected of testing a DN-3 ASAT missile capable of reaching higher orbits, with tests conducted in October 2015, December 2016, August 2017, and February 2018.[67] Although each of these tests cannot be verified, anonymous U.S. officials made statements asserting that the tests were of a new ASAT capability.[68] China may be developing three or more direct-ascent ASAT systems simultaneously, but it is not clear if each is intended to become operational or if some are intended to be missile interceptors.[69]

China has also developed and launched several satellites for testing technologies which could be used as co-orbital counterspace capabilities, however none of these tests have resulted in a verifiable destructive incident. Co-orbital satellite capabilities can serve a dual-purpose role as both on-orbit servicing and inspection satellites for peaceful purposes and as counterspace threats—and it is difficult to distinguish between the two.

For example, in 2008 a Chinese spacecraft deployed a miniature imaging satellite, called BX-1, that was jettisoned from its mother spacecraft. The satellite was unable to be actively controlled until after it

New Heights for China's ASAT Program

IN MAY 2013, China launched a new type of ASAT system, which Beijing claimed was intended to reach a height of 10,000 km and disperse a barium cloud for scientific research.[60] Although China claimed the test used an SC-19, experts deduced that the altitude reached was far beyond SC-19 capability.[61] According to the U.S.-China Economic and Security Review Commission, this test in fact used a new DN-2 rocket. After the test, the United States suggested that this test was likely a high-altitude direct-ascent ASAT test that could reach satellites as high as GEO, which includes satellites used for missile warning, military communications, GPS, and ISR.[62]

> "China is employing more sophisticated satellite operations and is probably testing dual-use technologies in space that could be applied to counterspace missions."
>
> U.S. DEFENSE INTELLIGENCE AGENCY[70]

had passed near the International Space Station (ISS).[71] However, many reports in the United States claimed that this was the first co-orbital ASAT test from China. While the BX-1 did fly dangerously close to the ISS, the maneuver appears to be unintentional.[72]

In 2010, China launched a satellite, designated SJ-12, which conducted a series of remote proximity maneuvers with an older Chinese satellite, SJ-06F. "The maneuvers occurred over several weeks between June 12, 2010, and August 16, 2010, and indicated a very slow and methodical approach."[73] Some have speculated that this mission was designed to test co-orbital jamming or other counterspace capabilities.[74] 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."[75] Although this may have been a test run for the 2011 docking of the Shenzhou space capsule with the *Tiangong*-1 space station, the SJ-12 maneuver could have serious counterspace implications as well.[76]

In July 2013, China placed three separate satellites into similar orbits. At the time, China claimed that the satellites were "conducting scientific experiments on space maintenance technologies."[77] 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. This maneuver has yet to be verified from publicly-available information.[78]

In June 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 space debris and remove it from orbit. Though studies on the incident debate the success of this test, the technology could potentially be further developed and used to damage or disable other satellites.[79] On that same mission, China also deployed the *Tianyuan*-1 spacecraft, which according to Chinese press accounts, successfully tested the ability to refuel other satellites while in orbit.[80] Both tests received significant media coverage in the U.S. due to their potential dual-use as ASAT weapons.

While none of China's rendezvous and proximity operations (RPO) activities in LEO or GEO appear to have damaged other satellites, these technological advancements have many experts concerned about their intent.

China can also pose a threat to space systems through its ability to attack the ground stations that control them with conventional forces. China has the largest standing army of any nation and over the past decade, has significantly increased its military budget and modern-

Figure 2: Chinese rendezvous and proximity operations in the geosynchronous belt. Publicly available data suggests that Chinese satellite SJ-17 made several close approaches in GEO. The figure below highlights several satellites that appear to have experienced close approaches with SJ-17 between April 2017 and February 2018. Learn more at aerospace.csis.org/sj17.

SPACE-TRACK.ORG

Inspecting the GEO Belt

IN NOVEMBER 2016, China tested RPO activities between two Chinese satellites in GEO. On the maiden launch of the Long March 5, it carried an experimental satellite designated SJ-17 into geostationary orbit.[81] SJ-17 later went on to approach a Lockheed Martin-built Chinese communications satellite, Chinasat 5A. SJ-17 circled nearby Chinasat 5A several times before remaining in a nearby orbit.[82] SJ-17 restarted maneuvers around the GEO belt in April 2017, visiting another Chinese satellite designated Chinasat 6A, and continued RPO activities with Chinasat 20, through April 14, 2018.[83] SJ-17 has not continued RPO activities since August 2018.

ized its conventional military forces.[84] 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, the U.S. Director of National Intelligence stated 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."[85] In 2019, the DIA 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."[86] Moreover, Chinese military and technical writings often reference directed energy as a key technology in a successful counterspace strategy.[87]

In 2005, several Chinese scientists claimed to have successfully blinded a satellite in a test using a "50-100 [kilowatt] capacity mounted laser gun in Xinjiang province."[88] However, this claim has not been confirmed through publicly-available information.

In 2006, reports surfaced that U.S. imagery satellites were illuminated by lasers over Chinese territory.[89] Though much speculation surrounded these incidents, senior United States officials have stated that "China not only has the capability [to blind satellites], but has exercised it."[90] Indeed, 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."[91] This incident demonstrates that China has much of the technology necessary to field an operational capability to dazzle or blind a satellite; and experts believe China will continue to work on developing efficient and accurate high-powered laser systems.[92] 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."[93]

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. This technological advance indicates that "China could have a mobile HPM system capable of attacking electronics on aircraft and anti-radiation missiles."[94] 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.

CHINESE MILITARY AND TECHNICAL WRITINGS OFTEN REFERENCE DIRECTED ENERGY AS A KEY TECHNOLOGY IN A SUCCESSFUL COUNTERSPACE STRATEGY.

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 indiscriminate damage to satellites, creating a high level of radiation in LEO that could last for years.[95] Although China has the technology necessary to field a nuclear-armed ASAT weapon, it appears to be focusing its efforts in other areas.

Electronic

China acquired foreign ground-based satellite jammers from Ukraine in the late 1990s, and has continued to develop the technology independently in the ensuing decades.[97] 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.[98] The DIA claims that China is developing jamming technologies to target SATCOM over a large range of frequencies, including several military protected communication bands.[99]

Non-military sources give further insight into Chinese focus on electronic warfare. A paper from the China Electronic Technology Group Corporation proposed

> Electronic warfare (EW) units within the PLA "routinely conduct jamming and anti jamming operations against multiple communication and radar systems and GPS satellite systems in force-on-force exercises."
>
> OFFICE OF THE SECRETARY OF DEFENSE[96]

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."[100] 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.[101]

At the DefCon hacking convention in Las Vegas in 2015, two Chinese researchers presented a guide to building a GPS spoofing device and sold kits for about $300.[102] Although there are no public accounts of the PLA spoofing GPS signals, the ability to spoof GPS and other satellite signals is well within the reach of the PLA, especially given the priority China places on electronic forms of attack.

China carried through with some of these plans, namely installing jamming equipment on the Spratly Islands. 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 targeting communications and radar. This assessment is supported by satellite imagery that shows a suspected jamming system on Mischief Reef. China has been building military installations across the island chain since 2014, but this is the first visual evidence of jamming equipment on these islands.[103] Shortly after the identification of the jammers, Vietnam condemned China's continued militarization and weaponization of the South China Sea and the Spratly Islands, stating that the jamming equipment violates international law.[104]

In June 2018, the *South China Morning Post* reported that China had made significant progress on an ionospheric radar, located on the island of Hainan, which also hosts China's newest spaceport—the Wenchang Satellite Launch Center—in the southeastern part of the country. The device, described as a high-powered incoherent scatter radar, is reported to "be capable of influencing the ebb and flow of subatomic particles as far away as Singapore, a distance of over 2,000 km (1,200 miles)."[105] Such a radar could disrupt signals from satellites, cutting off communications or access to satellite networks for those operating in the area. According to the same source, a Chinese scientist confirmed that the radar would be used for both civil and military applications.[106] Primarily, however, ionospheric radars are used in scientific experiments to learn more about the Earth's atmosphere.[107]

Satellite imagery of Mischief Reef in the Spratly Islands on May 6, 2018. Three tarp-covered truck-mounted jammers were placed on Mischief Reef in 2018. This type of jamming equipment will most likely affect ships and aircraft operating in the area.

DIGITALGLOBE / CSIS ASIA MARITIME TRANSPARENCY INITIATIVE

Cyber

China has highly advanced cyber capabilities, a majority of which are run by the SSF in conjunction with its counterspace operations. 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.[109] Chinese writings and research efforts indicate that in a conflict, it would attempt to conduct cyberattacks against U.S. satellites and ground stations.[110] 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

"These writings suggest that China is prepared to use cyber operations to manage the escalation of a conflict, as they view cyber operations as a low-cost deterrent and can demonstrate capabilities and resolve to an adversary."

OFFICE OF THE SECRETARY OF DEFENSE[108]

IN 2018 ALONE, CHINA TESTED TECHNOLOGIES IN THREE OF THE FOUR COUNTERSPACE WEAPON CATEGORIES.

logistics networks to affect the adversary's ability to operate during the early stages of conflict."[111]

China has already been implicated or suspected in several cyberattacks against U.S. satellites.[112] In October 2007 and again in July 2008, cyberattacks believed to have originated 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.[113] Each attack caused at least 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."[114]

In September 2014, Chinese hackers attacked the 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.[115] 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.[116]

Anonymous sources in India leaked that a "high-profile government meeting last month involving video chat via satellite was compromised by Chinese hackers" in October 2017. The video call 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 identify if the attack came from the Chinese government or non-state cybercriminals.[117]

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 Defense Department contractor and another private firm that sells geospatial imaging technology."[118] The researchers could not determine exactly which systems had been accessed in the breach, however 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 mainland China.[119]

SUMMARY

CHINA SHOWS NO SIGNS of slowing its investment in developing counterspace capabilities. Government and military officials often comment on how military space capabilities will ensure their success in conflict and create a significant advantage if China can interfere with the United States' reliance on space architectures. China is clearly investing in its counterspace capabilities. Evidence confirms that in 2018 alone, China tested technologies in three of the four counterspace weapon categories. Specifically, China has tested several direct-ascent ASAT weapons capable of reaching satellites in LEO and possibly GEO. China is also more frequently testing RPO capabilities that could lend themselves to a co-orbital ASAT system. Additionally, recent activities demonstrate that China is proliferating its electronic and cyber capabilities.

Number of Successful Orbital Launches in 2018[120]

19

RUSSIA

"Russia is developing a diverse suite of ground-launched and directed-energy ASAT capabilities, and continues to launch 'experimental' satellites that conduct sophisticated on-orbit activities to advance Russian counterspace capabilities."

U.S. MISSILE DEFENSE REVIEW[121]

BECAUSE OF THE SOVIET UNION'S DOMINANCE in the space domain during the Cold War—launching more payloads to orbit than all other countries combined—Russia remains a prominent space power today. Before the collapse of the Soviet Union in 1991, marking the end of the first global space age, the Soviets were driven to outperform the United States by reaching several key space technology milestones first.[122] The Soviet space agency placed the world's first satellite into orbit (Sputnik 1 in October 1957), achieved first contact with the surface of the Moon (Luna 2 in September 1959), and sent the first human into space (Yuri Gagarin in April 1961).

After its founding, the Russian Federation inherited three active Soviet spaceports: the Baikonur Cosmodrome, the Plesetsk Cosmodrome, and the Kapustin Yar Cosmodrome.[123] Since 1991, Russia has successfully launched space objects from three more facilities, including the relatively new Vostochny Cosmodrome in the country's far east, where it hopes to support human space launches in the future.[124] Unlike the Soviet Union, Russia is no longer responsible for the majority of global space launches. Although it achieved the greatest number of successful orbital launches of any country in 2014, Russia fell behind China and the United States in 2018 with only 19 launches to China's 38 and the United States' 34.[125]

Roscosmos—the Russian state corporation responsible for civil spaceflight—currently operates the world's most robust human space launch program. Since the end of the U.S. Space Shuttle program in 2011, the Soyuz launch system has been the only vehicle transporting astronauts to and from the ISS, fulfilling its partnership responsibilities as outlined in the Station's partnership agreements.[126] Russia was a founding partner of the ISS and is the second largest contributor to its construction and operation. Despite a deterioration in diplomatic and military relationships in recent years, Russia

The launch of Soyuz MS-11 to the International Space Station on December 3, 2018. This launch carried one Russian cosmonaut, one U.S. astronaut, and one Canadian astronaut. The Soyuz carried six foreign astronauts to the ISS in 2018.

KIRILL KUDRYAVTSEV / AFP / GETTY IMAGES

and the United States maintain a strong partnership in civil space, largely due to human spaceflight collaboration. The two nations share training, communications, operations, and launch capabilities in support of the ISS. Currently, NASA pays Roscosmos over $80 million each for seats aboard the Soyuz for American astronauts.[127] In 2018, Roscosmos flew three successful crewed missions (and one that was safely aborted before it reached orbit) carrying five Americans, four Russians, one Canadian, and one European.[128] According to budgetary data revealed during a January 2019 meeting between Russian president Vladimir Putin and Roscosmos director general Dmitry Rogozin, foreign revenue—including Soyuz seats sold to ISS partners—made up an estimated 17 percent of the corporation's total income in 2018.[129] The same document revealed the corporation ran deficits of approximately $156 million and $244 million in 2016 and 2017 respectively, but an estimated $29 million profit in 2018.[130]

Since the mid-2000s, Russia has embarked on a series of programs to modernize many of its languishing space capabilities. The Global Navigation Satellite System (GLONASS) constellation of PNT satellites deteriorated through the 1990s, dropping at one point to just nine functional satellites out of the 24 that are necessary for global coverage. In 2011, Russia began work on a third generation of satellites (GLONASS-K) that will greatly improve the accuracy and reliability of the system, and the constellation has now returned to the full complement of satellites necessary for global coverage.[132] Over the next decade, Russia plans to revamp its optical imaging satellites, land a scientific probe on the surface of Mars, and develop a new human launch system capable of placing cosmonauts in lunar orbit.[133] These missions will almost certainly require a significant budget increase for Russian civil space activities—an unlikely prospect according to some industry experts.[134]

SPACE ORGANIZATION AND DOCTRINE

THE RUSSIAN SPACE SECTOR is largely represented by two government organizations: Roscosmos, a state corporation

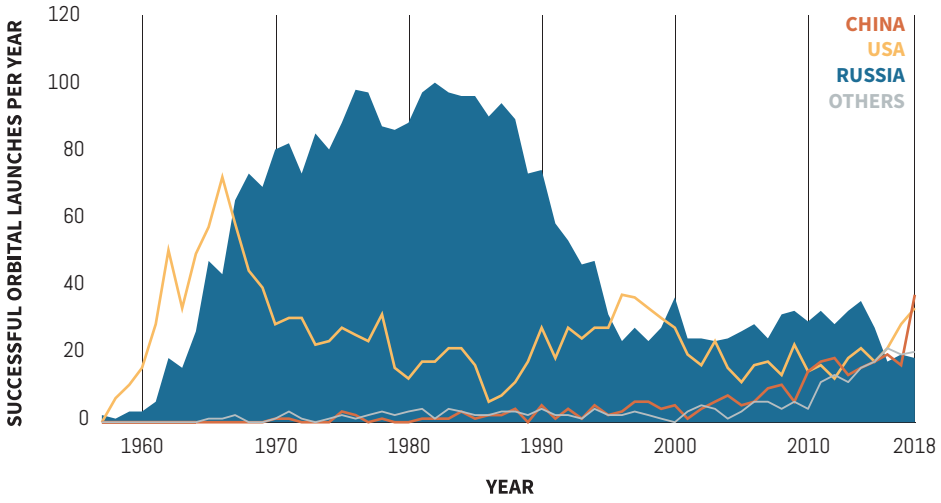


Figure 3: Russian orbital space launches (1957–2018). In the first space age, from 1957 to 1991, the Soviet Union completed more orbital space launches than any other space-faring nation. Since then, Russia's launch rate has fallen significantly, trailing behind the United States and China in 2018.

SPACE-TRACK.ORG / CSIS AEROSPACE SECURITY[131]

responsible for civil spaceflight, and the Russian Aerospace Forces, the branch of the Russian armed services tasked with military operations in the space domain. Roscosmos was formed in 2015, when two separate organizations—the Russian Federal Space Agency and the United Rocket and Space Corporation—were consolidated into one corporation tasked with "comprehensive reform of the Russian space industry" and the pursuit of international cooperation with space partners around the world.[135] In 1992, Russia became the first country to establish a space force—a branch of the Russian Armed Forces dedicated to space operations.[136] In 2015, after a series of military space reorganizations, the space force merged with the Russian air force—becoming the Russian Aerospace Forces.[137] The new Russian Space Forces sub-branch is responsible for launching military satellites, maintaining space-based assets, monitoring space objects, and identifying potential attacks against the Russian homeland from space.[138]

According to the Military Doctrine of the Russian Federation, last updated in December 2014, Russia considers the "intention to place weapons in outer space" a main external military danger.[139] To address this concern, the doctrine states that one of Russia's principal tasks is to establish "an international treaty on [the] prevention of placement of any types of weapons in outer space."[140] In 2008, Russia and China 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.[141] While the topic of preventing an arms race in space has garnered a lot of attention, few countries have been supportive of the proposal. The United States dismissed it as a "diplomatic ploy," but so far has not offered an alternative.[142] Before the doctrine's release, co-author General Yuri Baluyevsky, former First Deputy Minister of Defense, articulated Russia's need to develop defense systems that could both retaliate and preemptively strike an aggressor's space forces.[143]

Other Russian military leaders' public remarks have shed more light on Russian military doctrine in the space domain since the formal document was last released in 2014. Former Deputy Prime Minister Dmitry Rogozin—who is now the Roscosmos director general—has stated that Russia does not use satellites to damage other space objects.[144] Rogozin, a centerpiece in Russian space leadership, has also said that the United States' ballistic missile defense systems and space operations—which he regularly compares to the Reagan-era Strategic Defense Initiative or "Star Wars"—are a principal justification for Russia's need to develop domestic counterspace weapons.[145] More recently, the current First Deputy Minister of Defense Valery Gerasimov stated that the proposal to create a U.S. space force is in and of itself "a pretext for militarizing space."[146]

COUNTERSPACE WEAPONS

Kinetic Physical

Russia appears to be fielding several kinetic physical counterspace weapons—including both ground- and air-launched direct-ascent ASAT missiles and potentially several co-orbital ASATs—capable of threatening satellites in all orbital regimes. Although several of these programs resemble previous, Soviet-era ASAT systems, and likely benefit from the Soviet Union's rich history of developing and operating anti-satellite weapons during the Cold War, others may be much newer.

In December 2018, Russia conducted its seventh test of the PL-19/*Nudol* direct-ascent ASAT system.[147] 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.[148] 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 much greater flexibility to target LEO satellites with orbital inclinations above 40 degrees as they transit over Russian territory.[149] The PL-19/*Nudol* completed its first successful flight test in November 2015, after two unsuccessful attempts.[150] U.S. intelligence sources confirm that the system is indeed designed as an ASAT weapon, but some analysts disagree on whether the launches should be considered ASAT tests, since the PL-19/*Nudol* missile system is also an exo-atmospheric missile interceptor.[151]

Other missiles in the Russian arsenal that are not specifically designed to strike satellites can also reach objects in space. The existing S-300 and S-400 surface-to-air missiles are capable of "near space" activity, with maximum altitudes of 75 and 200 km respectively.[152] Production of a follow-on surface-to-air missile system, the S-500, reportedly began in March 2018.[153] Oleg Ostapenko, former Deputy Minister of Defense, once stated that the S-500 will be able to intercept "low-orbital satellites and space weapons."[154] The S-500 is expected to be capable of reaching air targets up to 600 km away—corresponding to orbital altitudes up to 300 km if launched directly upwards.[155] The new missile's first successful test in May 2018 reached an air target 480 km away.[156] Since the S-300, S-400, S-500, and the latest version of the PL-19/*Nudol* systems are launched using mobile platforms, the use of any of these systems to actually destroy a target on orbit would require a high-precision targeting capability that has yet to be demonstrated via a destructive test.[157]

In September 2018, a photographer posted a photo to an online forum for aviation enthusiasts depicting a variant of the Russian MiG-31 fighter jet carrying an unidentified missile.[158] One month later, CNBC reported that the missile was likely a "mock-up" of an air-launched ASAT weapon that could become operational as early as 2022, citing three sources familiar with U.S. intelligence on the matter.[159] 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.[160] 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.[161] Some experts have interpreted the confirmation as a revival of the Soviet-era 30P6 *Kontakt* program. Although the *Kontakt* program was also supported by the MiG-31 aircraft, it used a different missile than the one photographed in September 2018.[162]

Historically, the Soviet Union's principal anti-satellite programs—which targeted satellites in both LEO and GEO—were co-orbital. The oldest co-orbital ASAT program—*Istrebitel Sputnikov* (IS), meaning "satellite destroyer" in Russian—completed 20 tests from 1963 to 1982, and successfully destroyed several of its

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

RUSSIA'S NEWEST CO-ORBITAL SYSTEM MAY BE DESIGNED TO TARGET SATELLITES IN GEO.

targets on orbit.[163] A modified version of the IS system, named IS-MU, became operational in 1991.[164] Like its predecessor, the IS-MU program was only designed to target satellites in LEO. The program officially ended in August 1993.[165]

In the early 1980s, the Soviet Union began developing its most powerful anti-satellite weapon to date, known as the *Naryad*. Also a co-orbital ASAT, the *Naryad* may have been designed to reach altitudes as high as 40,000 km, and could contain multiple individual warheads in a single launch, posing a serious threat to satellites in GEO.[166] The *Naryad* system's original upper stage—now called Briz-K—is still in use today as part of the commercial Rokot and Briz staging combination.[167] The *Naryad*-era ground station—named *Okno*, meaning "window" in Russian—can track space objects in MEO and GEO. Although *Okno* is in modern-day Tajikistan, control of the facility was transferred to Russia in the mid-2000s and it remains operational.[168] The system has undergone upgrades, and a 2016 report suggests that *Okno* can now detect objects as high as 50,000 km (well past the geostationary belt).[169]

New analysis published in *Jane's Intelligence Review* in September 2018 suggests that Russia's newest co-orbital system may be designed to target satellites in GEO.[170] Designated *Burevestnik*—a commonly-used name for Russian defense systems, meaning "stormy petrel"—the new co-orbital ASAT system is likely connected to a recent Russian RPO observed with suspicion by the international space community over the past five years.[171] The on-orbit inspection component of the *Burevestnik* system appears to share greatest similarity with Russian RPO activities in LEO in 2017 and 2018, including the use of relatively lightweight satellites for close approaches.

Suspicious RPO activity has also been observed in at least one Russian satellite in GEO.[176] The satellite—known as *Olymp-K*, but misleadingly referred to as Luch by the Russian government—has attracted attention for shifting its position within the geosynchronous belt on a relatively frequent basis, occupying at least fourteen different positions since its launch in September 2014.[177] *Olymp-K* first attracted attention when it repositioned itself between two satellites operated by Intelsat, a U.S. satellite communications company.[178] The two Intelsat satellites were separated by approximately 0.2 degrees of longitude in the geostationary belt, likely occupying the same orbital slot.[179] Approaching satellites in GEO in this manner could allow for close inspection or potentially intercepting their communication links.[180] Kay Sears, an Intelsat executive, expressed her concern over the issue and highlighted the Russian satellite's behavior as "not normal."[181] Although U.S. Space Command sent warnings to Russia after it predicted that *Olymp-K* would soon pass within 5 km of another satellite, Russia appeared unresponsive and later dismissive.[182] In September 2015, *Olymp-K* approached a third Intelsat satellite.[183] The international response escalated in September 2018, when French Minister of the

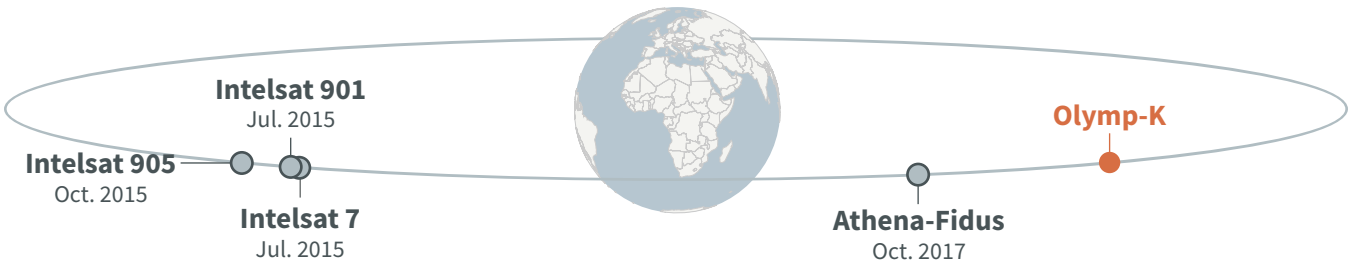
Figure 4: Russian rendezvous and proximity operations in the geosynchronous belt. Publicly available data suggests that Russian satellite *Olymp-K* made several close approaches in GEO. The figure below highlights several satellites that have experienced close approaches with *Olymp-K* between July 2015 and October 2017. Learn more at aerospace.csis.org/olymp.

SPACE-TRACK.ORG

Russian Nesting Satellites

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.[172] 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.[173] 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 August 2018, Assistant U.S. Secretary of State for Arms Control, Verification, and Compliance Yleem Poblete expressed concern over Russian RPO activity, calling it "very abnormal behavior."[174] Although secretive subsatellite deployments are indeed uncommon, space security experts disagreed with the U.S. State Department official, saying that RPO activities like the ones observed by Cosmos 2519 and its subsatellites are not inherently "nefarious or suspicious."[175]



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. For more details on *Olymp-K*'s movements in GEO, see Figure 4.

With the most diverse ballistic and cruise missile arsenal in the world, Russia poses a significant counterspace threat to satellite systems through its ability to strike satellite ground stations around the world with conventional forces.[184]

Non-Kinetic Physical

Russia likely has the capability to destroy and degrade satellites in space using non-kinetic physical counterspace systems, including high-altitude EMPs and directed energy weapons. Though perhaps not intentionally intended as ASAT weapons research, the Soviet Union first tested a non-kinetic counterspace weapon in 1961 and 1962, when it detonated three nuclear warheads approximately 400 km above the Earth's surface—including one over Kazakhstan, which destroyed the region's electrical grid.[185] Like the United States after the Starfish Prime test in 1962, the Soviets quickly learned of the indiscriminate damage of high-altitude nuclear tests and soon began working on other, kinetic physical weapons with more localized effects.[186] In April 1999, Vladimir Lukin, chairman of the Duma International Affairs Committee, told a U.S. congressman during an official visit that Russia had retained the Soviet Union's capability to detonate a high-altitude nuclear weapon.[187]

More recently, Russia appears to have renewed its Soviet-era directed energy counterspace weapon development and testing, including air- and ground-based laser weapons. In 2010, Russian news agency Interfax reported the development of a laser ASAT weapon for use aboard a modified *Ilyushin* Il-76MD cargo plane, known as the *Beriev* A-60.[188] The system—known as *Sokol Eshelon*, meaning "Falcon Echelon"—appears to be a revival of a Soviet system first developed in 1965.[189] Leaked photos of the aircraft from 2011 show a vertically-oriented laser mounted on the top of the plane. The laser system was reportedly used in 2009 to illuminate a Japanese satellite at an altitude of 1,500 km.[190] Although a 2012 report said the program was halted in 2011 due to budget cuts, a second Russian news report from the same year claimed the program is still operational.[191]

RUSSIA LIKELY HAS THE CAPABILITY TO DESTROY AND DEGRADE SATELLITES IN SPACE USING NON-KINETIC PHYSICAL COUNTERSPACE SYSTEMS.

In February 2018, Interfax reported that Russian weapons manufacturer Almaz-Antey had finished construction for a new laser ASAT weapon system with both ground- and air-based components.[192] Although the new system could be considered a follow-on to *Sokol Eshelon*, the Interfax report explicitly stated that the new laser weapon program would most likely rely on a "fundamentally new aircraft [that is] not based on the Il-76MD."[193] An aircraft-mounted laser weapon could be capable of dazzling or blinding sensors on satellites. If they are capable of higher power levels, they could also potentially degrade other light- or heat-sensitive physical components on a satellite, such as solar arrays, causing more permanent damage.

In September 2018, analysis published in *Jane's Intelligence Review* suggested that a component of the *Krona* laser space surveillance system less than 40 km north of the Georgian border may be upgraded to become a laser ASAT weapon.[194] Since 2005, the *Krona* facility has used laser ranging—sending short laser pulses to a satellite in order to observe the pulses' deflection and determine the distance between it and the observation site—to track space objects.[195] Similarly, Russia also has a robust network of ground-based lasers that are ostensibly for scientific purposes as part of the International Laser Ranging Service (ILRS), which has stations located all over the world.[196] Although there is no evidence showing that these lasers have been used to dazzle satellites, some of the same technologies used for laser ranging could be adapted for a counterspace system.[197]

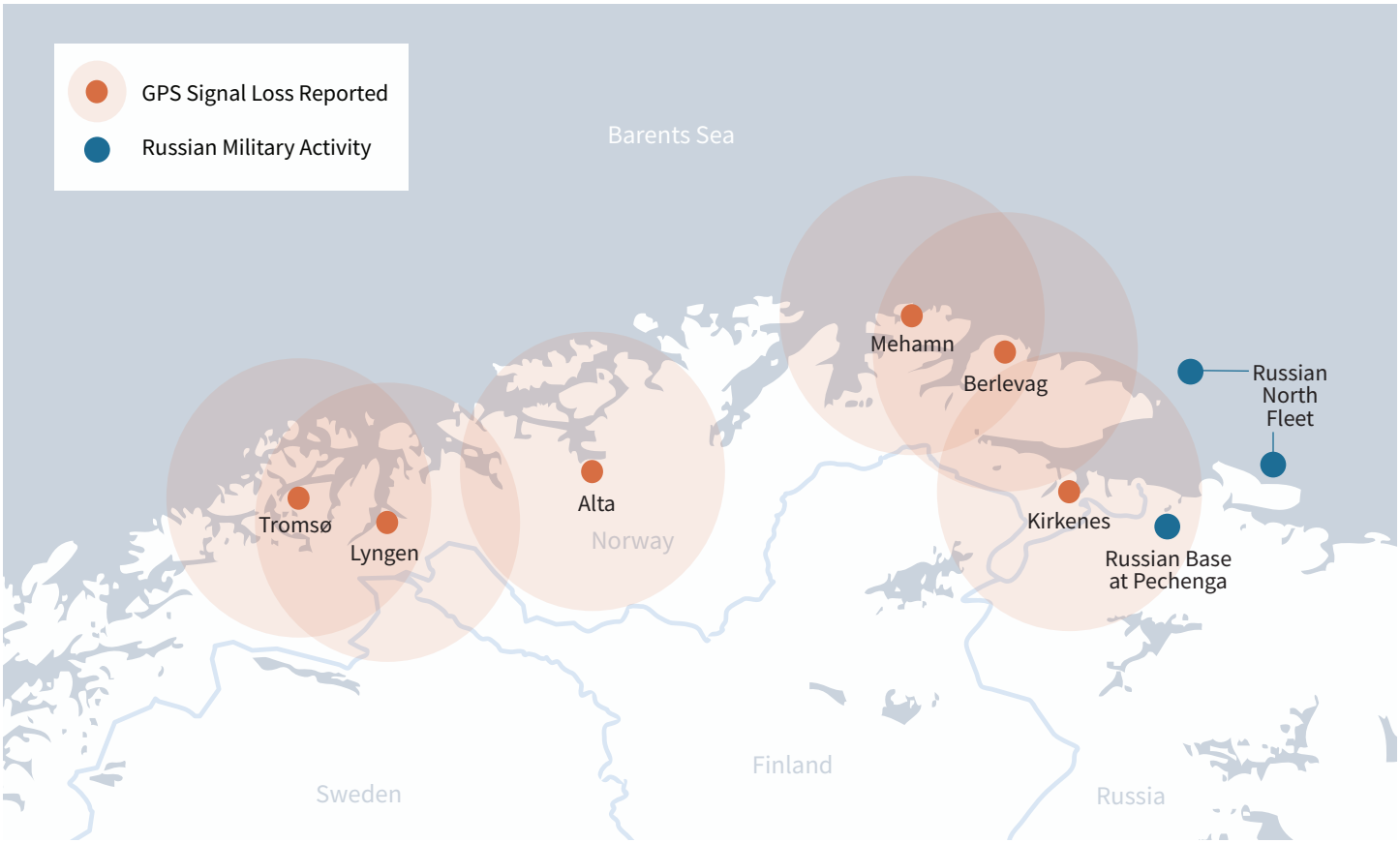


Figure 5: Instances of GPS Jamming in the Arctic Circle. Civilian airports in northern Norway and Finland have experienced periodic GPS outages that appear to correspond with military exercises happening in the region. Learn more at aerospace.csis.org/arcticjamming **THE BARENTS OBSERVER / THE GUARDIAN**

"There is a tendency nowadays to accuse Russia of all sins, mortal or otherwise...as a rule, these accusations are baseless."

DMITRY PESKOV, PRESS SECRETARY FOR THE PRESIDENT OF RUSSIA[198]

Electronic

Russia is regularly accused of aggressive GPS jamming and spoofing campaigns, affecting conflict regions like Ukraine and Syria during Russian interventions, and also bordering states like Norway and Finland during peacetime. These accusations are supported by strong evidence. During the Crimean conflict in 2014, Russia jammed GPS signals in Ukraine, which resulted in the loss of GPS for radios and phones, as well as the grounding of some remotely piloted aircraft. According to independent reports from Ukrainian analysts, Russia used six different jamming and radio monitoring platforms in Ukraine from 2014 to 2017, including the R-330Zh jammer and the R-381T2 ultra-high frequency (UHF) radio monitoring system.[199] In December 2018, Ukrainian Navy Commander Ihor Voronchenko accused Russia of jamming Iridium communication satellite signals and spoofing GPS during the Kerch Strait incident a month earlier—during which the Russian coast guard opened fire on three Ukrainian Navy ships.[200]

A video leaked in 2015 confirmed Russia's deployment of the *Krasukha*-4 truck-mounted jamming system in Syria. Reports also indicate that Russia supplied the Assad regime with R-330P jammers of its own.[201] In April 2018, NBC news reported that more recent Russian jamming in Syria has affected small U.S. drones operating in the region, citing four anonymous U.S. officials.[202]

For a week in September 2017, Widerøe—one of Norway's largest regional airlines—suffered a loss of GPS signals in the northernmost region of the country.[203] Analysis by the Norwegian National Communications Authority suggests that the

signal disruptions originated from the east, where Norway's Finnmark County borders Russia's Murmansk Oblast.[204] The affected week coincided with a Russian-Belarusian joint military exercise in Murmansk called *Zapad*-2017.[205] A year later, in October and November 2018, Norway hosted the North Atlantic Treaty Organization's (NATO) Trident Juncture 18 exercise in its eastern and central region—well south of Finnmark—using northern airports in Norway, Sweden, and Finland for supporting aircraft participating in the exercise.[206] Soon after the exercise, NATO spokesman Oana Lungescu announced that "Norway has determined that Russia was responsible for jamming GPS signals in the Kola Peninsula during Exercise Trident Juncture."[207] Several prominent Russian officials adamantly denied the accusations.[208] In January 2019, the northern Finnmark region of Norway again experienced GPS jamming during Exercise Clockwork, a British training exercise in Norway using Apache attack helicopters.[209] For more details on Russian jamming in the Arctic Circle, see Figure 5.

In June 2017, the U.S. Maritime Administration reported an apparent GPS spoofing attack in the Black Sea.[210] A ship operating near Novorossiysk, Russia, measured a 30 mile error in its GPS fixing position. Over 20 other ships in the region reported similar issues.[211]

Although the majority of electronic attacks attributed to Russia primarily affect relatively small regions, Russia may also be developing the capability for more widespread GPS jamming across its territory. In 2016, the Russian military began installing GPS jammers, a system called *Pole*-21, on each of the country's 250,000 cell phone towers. Each *Pole*-21 system has an effective range of 80 km.[212]

Cyber

Russia's cyber capabilities are among the most advanced in the world. Since 2007, a Russian-speaking group of hackers—likely linked to the Russian government—has used malware called Turla to hijack older commercial satellite internet services that still use unencrypted data links as part of their command and control infrastructure.[213]

Outside of the space domain, Russia is regularly accused of engaging in cyberwarfare. In 2007, Russia was blamed for cyberattacks against Estonia which paralyzed online banking services, government communications, and Estonian media outlets.[214] Similarly, Ukraine has sustained thousands of Russian cyberattacks throughout the Crimean conflict over the past few years.[215] In 2015, a French satellite TV network was pulled off the air in an attack linked to a Russian hacker group known as APT 28.[216] In 2017, four U.S. intelligence agencies assessed with "high confidence" that Russia interfered with the 2016 presidential election using a variety of cyberattacks and social engineering schemes.[217] The governments of the United Kingdom, France, Germany, Kyrgyzstan, and Georgia have each accused Russia of similar cyberattacks. Given Russia's prolific use of cyberattacks in other domains, Russia's cyber capabilities likely pose a significant threat to space systems as well.

SUMMARY

OVERALL, RUSSIA POSES a significant threat across all four counterspace weapon categories. Evidence suggests that the country is currently developing TEL- and air-launched direct-ascent ASAT weapons, co-orbital systems for on-orbit inspection, ground- and air-based laser weapons, and a world-class network of electronic weapons. Russia is likely also capable of destructive cyberwarfare targeting satellite systems and the ground stations that support them. Although a large portion of the country's counterspace programs has been inherited from the Soviet Union, recent activities observed in the unclassified domain make it clear that developing a robust, diverse arsenal of counterspace weapons is a priority for the modern-day Russian Federation.

Number of Successful Orbital Launches in 2018[218]

0

IRAN

"Iran's regional ambitions and improved military capabilities almost certainly will threaten US interests in the coming year."

DANIEL R. COATS, U.S. DIRECTOR OF NATIONAL INTELLIGENCE[219]

IRAN'S PURSUIT OF SPACE CAPABILITIES is a relatively recent development, and its efforts in space are often viewed as a thinly-veiled cover for its developing ballistic missile program.[220] Iran has a relatively weak space industrial base, especially given the Iranian Space Agency's close ties to the nation's Ministry of Defense, and evidence suggests that a portion of Iran's space technologies were adapted from Russian and North Korean counterparts.[221] Iran maintains a domestic space launch facility in the northeastern Semnan Province, and in 2014, it also secured an agreement to use the Russian-owned Baikonur Cosmodrome Cosmodrome in Kazakhstan for space launch.[222]

Iran successfully launched its first domestically-manufactured satellite on a *Safir*-1 rocket in February 2009, and has vowed to put a human in space by 2025.[223] While human spaceflight remains a stretch for Iran, the space agency claims to have sent various living creatures into space in recent years, including a monkey in 2013.[224] In January 2019, Planet, an Earth imaging company, released images of two new Iranian space launch pads at the Imam Khomeini Space Center.[225] One of these pads was the launch site of a failed launch attempt on January 15, 2019. According to press reports, "Iran's information and communications minister, Mohammad Javad Azari Jahromi, announced on social media that the rocket failed to reach the speed needed to enter orbit around the Earth due to a failure in the launcher's third stage."[226] The *Simorgh*, the space launch vehicle used in this test, has yet to complete a fully successful mission, despite several attempts.[227]

The U.S. intelligence community has concluded that Iran's continued work to develop space launch vehicles will shorten the timeline to create a successful ICBM since the two systems use similar technologies.[228] After the January launch attempt, Israeli president Benjamin Netanyahu claimed the launch was, in fact, a test of the first stage of an ICBM.[229] A few days

A replica of the Iranian *Safir* launch vehicle on display on February 10, 2009. The *Safir*-1 launch vehicle has a 50 percent success rate.

SCOTT PETERSON / GETTY IMAGES

prior to the test, U.S.secretary of state, Mike Pompeo, made a similar statement, asserting that tests of Iran's space launch vehicle program include "virtually identical" technology as a ballistic missile and are a violation of the 2015 nuclear deal.[230]

Experts noted that a second launch was attempted on February 6, 2019 by a *Safir*-1 launch vehicle. Images released by Planet showed preparation activity for the launch on February 5, "including people and launch vehicles at the site, the two-stage *Safir* rocket and a truck with possible propellant tanks."[231] On February 6, images showed burn marks on the pad—a tell-tale sign of a launch—but Iran has not claimed to have successfully placed a satellite in orbit.[232] Reports speculate the payload on board was a remote-sensing satellite developed by the Sharif University of Technology.[233] Experts assess that something must have gone awry in the second stage or deployment of the satellite into its intended orbit, since Iran did not publicly announce a successful launch or the placement of a satellite into orbit.[234]

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. According to the Iranian defense minister Ahmad Vahidi, "[t]he base is aimed at securing the country's space facilities and monitoring space objects, especially satellites that pass overhead."[235]

SPACE ORGANIZATION AND DOCTRINE

IN 2003, IRAN FORMED the Iranian Space Agency to coordinate its space activities and technology development. The space agency is in charge of both military and civil space programs, and the distinctions between the two have at times been blurred.[236] The agency is under the oversight of the Ministry of Information and Communications Technology, but it takes direction from the Supreme Space Council. The Supreme Space Council is chaired by the president of Iran and is presided over by the defense minister.[237] The head of the Iranian Space Agency serves as the secretary of the Supreme Space Council.[238] 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.[239]

EVIDENCE SUGGESTS THAT IRAN BELIEVES THE CAPABILITY TO DENY THE UNITED STATES THE ABILITY TO USE SPACE IS CRITICAL TO ITS SECURITY.

Iran's military spending has expanded by over 50 percent in the last five years, swelling to 7.5 percent of its total budget for 2018–2019.[240] Though Iranian leadership takes steps to obscure the specifics of its budget, priorities include improving domestic missile production capabilities, which are currently limited due to Iran's reliance on imported missile engines. Traditionally, Iran's military doctrine has included using its ballistic missile capabilities to respond to attacks by striking large targets, an activity limited by its arsenal's poor accuracy. Evidence shows that Iran hopes to continue development focused on precision targeting.[241] While Iran is not a major space power in terms of its space capabilities, it has developed significant counterspace capabilities that can threaten U.S. space systems.

COUNTERSPACE WEAPONS

Kinetic Physical

Open-source information does not indicate that Iran is attempting to develop either direct-ascent or co-orbital ASAT weapons; however, Iran has the ballistic missile technology necessary to form the basis of a future direct-ascent kinetic ASAT capability. Iran has developed, tested, and proliferated a wide range of ballistic missiles, including the *Shahab*-3, which is believed to be derived from the North Korean *No Dong* 1 missile,[242] and the *Safir*-2, which has been used as a space launch vehicle.[243] Iran has demonstrated the ability to launch and operate rudimentary satellites, and its space monitoring center gives it the ability to track objects and better understand the space environment. But many other technological hurdles would need to be overcome before it could field a direct-ascent kinetic ASAT weapon, such as onboard sensors that could guide a warhead into a target satellite.

Iran could construct a crude direct-ascent ASAT capability in the near-term by using existing ballistic missile technology to launch an unguided warhead within the vicinity of a target satellite. An unguided kinetic ASAT weapon is unlikely to be effective at striking a satellite directly, but it could create a debris hazard that threatens the safety of the target satellite and other satellites in a similar orbit, forcing them to maneuver and expend precious propellant.

In 2018, United States-based analysts discovered that Iran was bringing a long-thought defunct missile test site back online. This site is outfitted for long-range missile tests, which inherently could evolve into an ASAT capability, although there is no reason to think this is the intended purpose of these test sites.[244] To date, Iran has not tested or proven capabilities needed for a co-orbital anti-satellite weapon.

Iran can also pose a moderate threat to space systems through its ability to attack ground stations with conventional forces. Iran has fairly substantial conventional forces with an estimated 534,000 active personnel.[246] Certain aspects of their conventional forces could pose a kinetic physical threat, especially to accessible regional ground stations. For example, through a successful ground or sea-based attack, or a cruise or ballistic missile, Iran could hypothetically damage or destroy a U.S. ground station in Bahrain that supports GPS.[247]

Non-Kinetic Physical

Iran may have acquired and used a laser dazzling or blinding counterspace system

Tracking Iran's Launch Infrastructure

IRAN MAY ONCE AGAIN be developing and testing long-range missiles at a site that hosted a lone missile launch test in 2013, but has since been considered defunct. Recent satellite imagery of Shahrud, Iran, shows dramatic increases in facility infrastructure over the last few years, including buildings painted a vibrant hue favored by the former lead scientist of Iran's long-range missile program.

Though analysts determined that the majority of the Shahrud facility features underground structures, open-air evidence of missile activity is also apparent. Evident in the photos are highly specific signs of long-range missile testing such as prominent ground scars, a known result of missile test-fires. The scars appeared in 2016 and 2017 in front of missile stands capable of supporting engines with between 62 and 93 tons of thrust of power (enough thrust for an ICBM, or anti-satellite capability). If Iran is indeed working toward developing ICBMs, the process may take between 5 and 10 years.[245]

on a United States satellite. In 2011, the Christian Science Monitor quoted an unnamed European intelligence source stating that Iran managed to "blind" a U.S. satellite by "aiming a laser burst quite accurately."[248] 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 rather sophisticated. 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 pursue a breakout nuclear capability, it is conceivable that it could mate a nuclear weapon with one of its ballistic missiles to create a nuclear ASAT capability.[249] However, the U.S. Director of National Intelligence has publicly stated that Iran has not yet developed a nuclear weapon and the Joint Comprehensive Plan of Action (JCPOA) "has extended the amount of time Iran would need to produce enough fissile material for a nuclear weapon from a few months to about a year."[250] The aim of Iran's nuclear program all along has been to develop a nuclear-armed ICBM to deter the United States, not a nuclear counterspace ASAT weapon, so it is unlikely to pursue this capability in the foreseeable future.

Electronic

"Iran undertakes more purposeful interference with U.S. military and commercial space systems using lasers and jammers than any other country."

MICAH ZENKO,
COUNCIL ON FOREIGN RELATIONS[251]

Iran has an extensive record of using electronic forms of attack against space systems, including uplink jamming, downlink jamming, and spoofing. On July 16, 2003, Voice of America (VOA) broadcasts to Iran began to experience interference with their 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 the Cubans determined that the jamming was "by the Iranians in Cuba, using a compound in a suburb of the capital belonging to the Iranian embassy." Cuban authorities promptly shut down the Iranian facility and issued a note of protest to the Iranian government.[252] Similar attacks emanated from Bulgaria and Libya from 2005 to 2006.[253]

THE MOST CONCERNING ELECTRONIC ATTACK CAPABILITY IRAN HAS PUBLICLY CLAIMED IS ITS ABILITY TO SPOOF GPS SIGNALS.

In 2010, Iran jammed British Broadcasting Corporation (BBC) and VOA satellite downlink signals going into Iran. At first, the jamming targeted BBC and VOA broadcasts on the Hot Bird 6 commercial satellite; when the broadcasts were moved to other commercial satellites, the jamming targeted them as well.[254]

Perhaps the most concerning electronic attack capability Iran has publicly acknowledged is its ability to spoof GPS signals. In 2011, Iran claimed to have downed a U.S. RQ-170 drone by jamming its satellite communications links and spoofing the GPS signals it received. An Iranian engineer was quoted at the time as saying that they were able to make the drone "land on its own where we wanted it to, without having to crack the remote-control signals and communications."[255] The U.S. government did not verify Iran's claims, but if true, they represent a significant coun-

IRAN WAS SUPPORTED BY THE SYRIAN GOVERNMENT IN A COORDINATED JAMMING EFFORT AGAINST APPROXIMATELY 25 INTERNATIONAL BROADCASTERS.

terspace capability that could be used to thwart U.S. precision-guided weapons in the future.

Iran has also been jamming several international and regional television broadcasts in the Middle East. Al Jazeera faced targeted attacks in January 2012 after its coverage of the the conflict in Syria. The origin of the attacks were traced to two locations in Iran.[256] 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." This attack also affected Eutelsat broadcasts in Western Europe.[257]

Cyber

Iran is also believed to have advanced offensive cyber capabilities that could potentially be used to target U.S. space systems. Specifically, Iran is believed to be actively exploring the military uses of cyber capabilities to disrupt enemy missile defense systems, remotely piloted aircraft, logistics operations, and command and control links.[258] In the past, Iran has demonstrated its cyber capabilities by attacking U.S. infrastructure. In 2012, Iran launched a massive denial of service attack against United States banks and telecommunications companies. This particular incident prompted a public statement by then-defense secretary 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.[259]

In 2014, Iranian hackers "successfully compromised a Kurdish satellite television station, Newroz TV," which is aligned with the Kurdistan Workers' Party (PKK). Iranian cyber capabilities are growing and so is Iran's willingness to employ cyber attacks against targeted defense companies, media conglomerates, and adversaries.[260] Iran's sophisticated cyber capabilities suggest that it could employ cyberattacks on space systems as well.

SUMMARY

ALTHOUGH IRAN IS OPENLY investing in space launch capabilities, it is far from developing any direct-ascent kinetic physical ASAT weapon. Similarly, with only a few successful satellites in orbit, Iran is unlikely to develop co-orbital kinetic physical capabilities in the near future. To make significant quick progress on any kinetic physical system, Iran would likely need technology and resources from either from either Russia or China. The same may be true for Iran's kinetic non-physical capabilities. However, Iran has moderate electronic and cyber counterspace capabilities and has demonstrated successful jamming and hacking attacks in recent years.

Number of Successful Orbital Launches in 2018[261]
0

NORTH KOREA

"Pyongyang and Washington's position on their satellite launches are radically different, and thus a crisis may arise once again, and one cannot say it will not end up with a war."

CHEONG SEONG-CHANG, SEJONG INSTITUTE[262]

LIKE MANY SPACEFARING NATIONS, North Korea's space capabilities are closely tied to its ballistic missile development. The *Unha*-3—the space launch vehicle used for North Korea's only two successful orbital launches—likely used components from other missiles within the country's arsenal, including the medium-range *Nodong* and Scud-class ballistic missiles.[263] Although reaching orbit is a significant achievement, many experts doubt that the few satellites launched by North Korea perform all of the functions the North Korean government claims.[264] There is little indication that North Korea is making substantial efforts to build or sustain a space industrial base, but its missile program is growing and many believe that it is aided by technology from China, Iran, and Pakistan.[265]

Although North Korea has successfully achieved orbital space launch in the past, satellite imagery suggests that the nation's only active spaceport—the Sohae Satellite Launching Station on the country's western coast—was being actively disassembled in 2018.[266] In a press conference following the release of a joint declaration between the U.S. president and the North Korean leader, President Donald Trump stated that leader Kim Jong-un agreed to destroy "a major missile engine testing site."[267] While such a commitment was not included in the signed declaration, the North Korean government appeared to have selected Sohae.[268] More recent satellite imagery—acquired in March 2019—suggests that the North Koreans have sharply reversed their activities and are rapidly rebuilding the site.[269]

Satellite imagery of the Sohae Satellite Launching Station, January 20, 2019. The spaceport has not been used for an orbital space launch attempt since July 2016. Satellite imagery shows some dismantling activity between June and August 2018, but little since then.

DIGITALGLOBE / CSIS BEYOND PARALLEL

Before constructing the Sohae spaceport, North Korea attempted an orbital space launch in 1998 from the Tonghae Satellite Launching Ground—a launch facility on the country's east coast, well-positioned for eastward launches over the Sea of Japan—using a variant of the *Taepodong*-1, an intermediate-range ballistic missile.[272] Although North Korea claimed that a satellite reached orbit and broadcasted songs honoring North Korean leaders, U.S. Space Command later stated that no payload successfully reached orbit as a result of the launch.[273] The Tonghae launch site hosted two more failed launch attempts in 2006 and 2009.

North Korea suffered another failure in April 2012, this time using the *Unha*-3 at the Sohae spaceport. In December 2012, the country successfully orbited its first satellite.[274] In February 2016, it successfully placed a second satellite in orbit.[275] While the space capabilities provided by these two satellites have little, if any, military significance, it demonstrates that the nation has the capability of placing an object into orbit.

North Korea has been clear in the past about its plans to continue launching satellites.[276] In 2017, a South Korean newspaper reported that a new satellite was being prepared for launch.[277] The report suggested that the *Kwangmyongsong*-5—which uses the same name as all previous North Korean satellites—would be significantly more advanced than its predecessors, featuring remote sensing and communications capabilities. The satellite may be launched on a transporter erector launcher (TEL) as opposed to the previously successful *Unha* vehicle. Using a TEL would allow North Korea to use several of its dispersed missile operating bases—effectively launching a satellite unannounced—instead of the Sohae Satellite Launching Station, where an *Unha* rocket would be visible on the launch pad via satellite imagery prior to launch.[278]

In parallel with its space program, North Korea has also made significant progress in developing and testing ballistic missiles. After a significant increase in ballistic missile tests since leader Kim Jong-un's inauguration in 2011, reaching a peak of 25 launches in 2017, North Korea abruptly halted its test program and launched no missiles in 2018.[279] The most powerful missile tested thus far, the *Hwasong*-15, reached an altitude of almost 4,500 km during its test flight, higher than satellites in LEO.[280] Based on publicly available information, however, it is not clear whether North Korea has developed the re-entry vehicle technology that would be necessary to deploy a conventional or nuclear warhead on its long-range missiles.

Disassembling a Spaceport

ACCORDING TO A JANUARY 2019 report from the Center for Strategic and International Studies' Beyond Parallel program, the Sohae Satellite Launching Station showed "some initial steps" of disassembly in the two months following the 2018 Singapore Summit meeting between U.S. president Donald Trump and North Korean leader Kim Jong-un, but little evidence of any additional dismantling activity after August 2018.[270] A second CSIS Beyond Parallel report showed images from March 2019—just two days after President Trump and the North Korean leader met at the Hanoi summit—showing rapid rebuilding activities at Sohae.[271]

SPACE ORGANIZATION AND DOCTRINE

LITTLE IS KNOWN about North Korea's doctrine or operational concepts for the use of counterspace capabilities. It has been noted that the absence of discussion about counterspace capabilities that could threaten the U.S. military is curious given the aggressive rhetoric used by the regime in touting its nuclear and missile programs.[281]

In March 2009, North Korea became a signatory to two United Nations space treaties: the Outer Space Treaty of 1967 and the Convention on Registration of Objects Launched into Outer Space of 1974.[282]

Four years later, in April 2014, the country's Supreme People's Assembly established the National Aerospace Development Administration (NADA), the official North Korean space agency.[283]

In public remarks, representatives from North Korea's delegation to the United Nations aggressively assert their state's right to pursue peaceful space operations that benefit its technological development and improve the quality of life for its citizens.[284] But due to the means by which the country reaches space—hitching a ride onboard a launch system clearly derived from a ballistic missile—North Korean space activities are constantly at odds with UN Security Council resolutions prohibiting missile development.

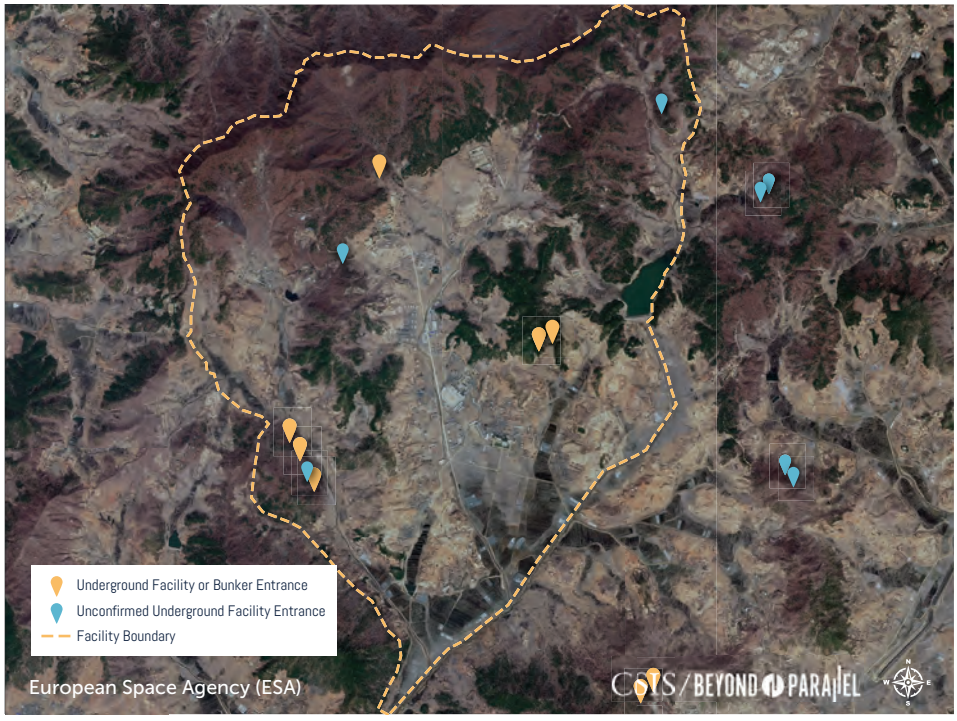
COUNTERSPACE WEAPONS

Kinetic Physical

To date, North Korea has not tested, or indicated that it is attempting to develop, a direct-ascent or co-orbital ASAT capability. The space launch and ballistic missile technology demonstrated by North Korea could serve as the basis for a kinetic ASAT capability, but many technological hurdles remain. An effective direct-ascent or co-orbital ASAT weapon would require onboard sensors—optical, infrared, radar, etc.—and a guidance system to steer the warhead into a target satellite. There are no indications that North Korea has or is attempting to acquire the technology needed for this.[285] It is conceivable that North Korea could field a crude direct-ascent ASAT capability in the near-term by adapting a ballistic missile to launch an unguided warhead to detonate in the vicinity of a target satellite. Such a weapon would be unlikely to directly strike a satellite, but it could create a debris field that complicates future operations for the target satellite and any other satellites in a similar orbit.

In 2018, the Center for Strategic and International Studies' Beyond Parallel program released a report identifying undeclared missile operating bases in North Korea, which could be used for TEL launches in a crisis scenario.[286] One newly identified site—the Sino-Ri missile operating base pictured below—is equipped with *Nodong*-1 medium-range ballistic missiles (MRBM).[287] A missile of this class would likely be able to carry a 1200 kg payload to a maximum altitude of 600 to 750 km, well within the LEO orbital regime.[288]

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.[289] Although North Korea's missile technology has developed quickly over the last 15 years, it is unlikely that the country could threaten ground stations at long distances, due to the limited range and accuracy of its ballistic and cruise missile arsenal.[290]



Satellite imagery of the Sino-Ri missile operating base on April 4, 2018. The facility likely hosts *Nodong*-1 MRBM, a TEL-launched missile capable of reaching LEO if used in a direct-ascent ASAT scenario.

DIGITALGLOBE / CSIS BEYOND PARALLEL

Non-Kinetic Physical

Some evidence suggests that North Korea may be developing the capability to deploy a nuclear EMP. However, the technology necessary to develop other directed energy weapons, such as lasers that can dazzle or blind the sensors on satellites, requires a level of sophistication that North Korea likely does not possess.[291] A third country, such as China or Russia, could provide these capabilities to North Korea, but there is no publicly available evidence to suggest this has happened.

In a written statement to Congress in 2017, the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, commonly referred to as the EMP Commission, offered evidence that North Korea may be developing an EMP weapon, warning of a "potentially imminent and existential threat of nuclear EMP attack" against the United States.[292] The EMP Commission notes that in 2004 two Russian generals warned the commission that the design for a Russian EMP warhead was unintentionally transferred to North Korea. South Korean intelligence officials told the press in 2009 that Russian scientists were in North Korea helping to develop an EMP weapon. Moreover, the commission notes that in 2013 a Chinese military commentator indicated that North Korea already has "super-EMP nuclear weapons."[293] In 2018, The Daily NK—a South Korean news site—obtained a North Korean internal document describing the level of damage possible as a result of a nuclear EMP attack.[294] The material was originally distributed as part of a collection of propaganda celebrating the political platform of the Workers' Party of Korea, the ruling party of North Korea.

A 2017 U.S. DIA assessment concluded that North Korea has the capability to produce a nuclear weapon small enough to be launched aboard a ballistic missile.[295] Thus, North Korea could theoretically launch a nuclear weapon into space and detonate it.[296] Unlike an ICBM—which would require an accurate guidance system and a reentry vehicle to ensure the warhead reaches its target on the ground—a nuclear-armed missile aimed at destroying satellites in LEO could be detonated above the atmosphere, requiring significantly less advanced technologies.[297] Although North Korea is not a signatory of the 1963 Partial Test Ban Treaty, the country has never tested a nuclear weapon at high altitudes.[298]

The view from the North Korean mission control room on April 8, 2012, during the first *Unha*-3 launch. Although this launch did not successfully reach orbit, the same launch facility supported a successful orbital launch using the same launch system just eight days later.

PEDRO UGARTE / AFP / GETTY IMAGES

NORTH KOREA HAS REPEATEDLY USED ITS GPS JAMMING CAPABILITIES AGAINST SOUTH KOREA.

Electronic

North Korea has acquired and is actively using electronic forms of attack against space systems. In 2010, the 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 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.[299]

In the years since, North Korea has repeatedly used its GPS jamming capabilities against the South. More GPS jamming occurred in December 2010 and again in March 2011. The 2011 incident lasted 10 days and coincided with an annual

U.S.-Korean military exercise.[300] Jamming occurred again in April 2012, disrupting air traffic at Incheon and Gimpo International Airports, and forcing flights to use alternative navigation systems.[301] In March and April 2016, over 250 South Korean fishing boats lost access to GPS, forcing them to return to shore.[302] A few days later, South Korea complained to the United Nations 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.[303]

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."[304] The jammers are mounted on mobile platforms and are operated intermittently, so they could be difficult to locate and neutralize in a conflict. North Korea appears to be gaining operational experience using these systems in peacetime. To what extent these capabilities are integrated into its overall military operations remains unknown. Since 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. Despite South Korean protests to the United Nations that North Korea's GPS jamming is a violation of the 1953 armistice agreement, no effective measures have been publicly undertaken to date to curb this activity.[305]

Cyber

General Vincent Brooks, then-commander of United States Forces Korea, noted in congressional testimony that North Korea's well-organized and advanced cyber forces are perhaps among the best in the world.[306] South Korea's Ministry of National Defence reports that North Korea doubled its cyber warfare personnel from approximately 3,000 troops in 2013 to 6,000 in 2015.[307]

Under the Kim Jong-Un regime, North Korea has exercised its cyber forces frequently, launching attacks on South Korea, the United States, and others. In one of the most widely reported incidents, North Korea launched a cyberattack against Sony Pictures Entertainment in November 2014.[308] The following month, in a move that may have been intended to demonstrate the capability to damage physical infrastructure through cyberspace, North Korea conducted a cyberattack on a South Korean nuclear power plant.[309] In 2018, the U.S. Department of Justice unsealed its criminal charges against an individual North Korean citizen for stealing over $80 million from a Bangladeshi bank.[310]

Given its demonstrated cyber capabilities, it is conceivable that North Korea could initiate a cyberattack against U.S. space systems to intercept information, as it did in the Sony attack, or to inject corrupt information that could cause physical damage to U.S. satellites or the forces that depend on them.

SUMMARY

NORTH KOREA HAS ONLY DEMONSTRATED its capabilities in two of the four counterspace weapon categories: electronic and cyberattack capabilities.

Although North Korea has demonstrated its dedication to increasing the range of its ICBM-class missiles, its failures on-orbit—or in most cases, failures to reach orbit—suggest that the country is far from developing the capabilities needed to pose a significant kinetic physical threat to 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 all satellites in the target's orbital regime.

Number of Successful Orbital Launches in 2018[311]
21

OTHERS

"The security environment is becoming more complex with our adversaries' determined pursuit of advanced technologies across multiple domains to include cyber, space, and [weapons of mass destruction], expanding regional and global ambitions."

LTG ROBERT ASHLEY,
DIRECTOR OF THE U.S. DEFENSE INTELLIGENCE AGENCY[312]

ACTORS BEYOND CHINA, RUSSIA, IRAN, AND NORTH KOREA have developed or have laid the foundation for counterspace weapons and dual-use technologies. This chapter explores the demonstrated space and counter space capabilities of other countries, including some U.S. allies and partners, along with changes in doctrine, infrastructure, and financing that might contribute to counterspace capabilities in the future.

EGYPT

IN 2018, EGYPT SIGNALED its intent to invest more heavily in space by establishing the Egyptian Space Agency.[313] The Egyptian Space Agency's primary objective is to manufacture and launch satellites. The agency plans to "develop and transfer space science and technology into Egypt to build satellites and launch them from Egyptian territories."[314] On February 21, 2019, EgyptSat-A was launched from Russia on a Soyuz rocket and placed into LEO.[315] EgyptSat-A is Egypt's third remote-sensing satellite and was jointly developed by Egypt's National Authority for Remote Sensing and Space Sciences together with RKK Energiya, a Russian satellite and rocket company.[316]

In addition to developing its own domestic space capabilities, Egypt has demonstrated some counterspace capabilities in recent years. In 2013, the Qatar-based news organization Al Jazeera reported that its satellite signals were being jammed by Egyptian authorities in order to block the news site from reporting on the military takeover of the government. The operation targeted Arabsat, a satellite owned by the Arab League, and NileSat, Egypt's own satellite.[317] The company was forced to change frequencies several times to avoid the jamming. According to Al Jazeera, it traced the jammers

OTHERS

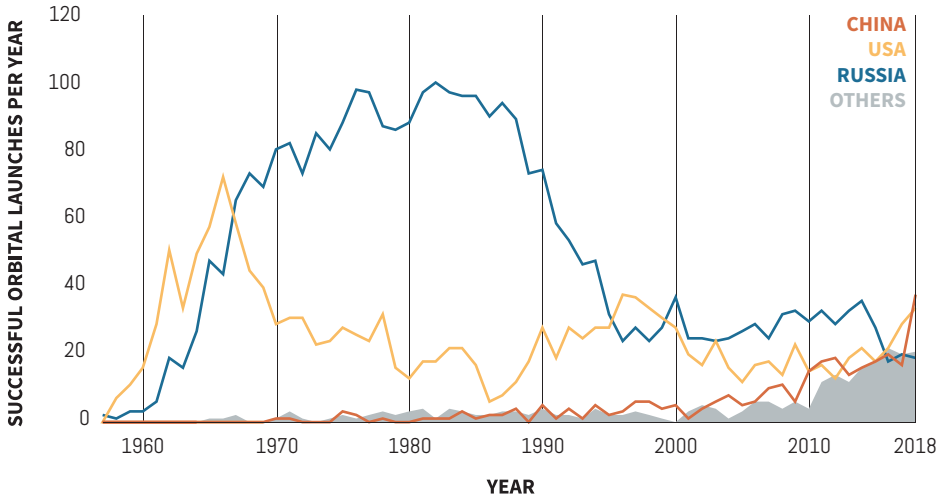
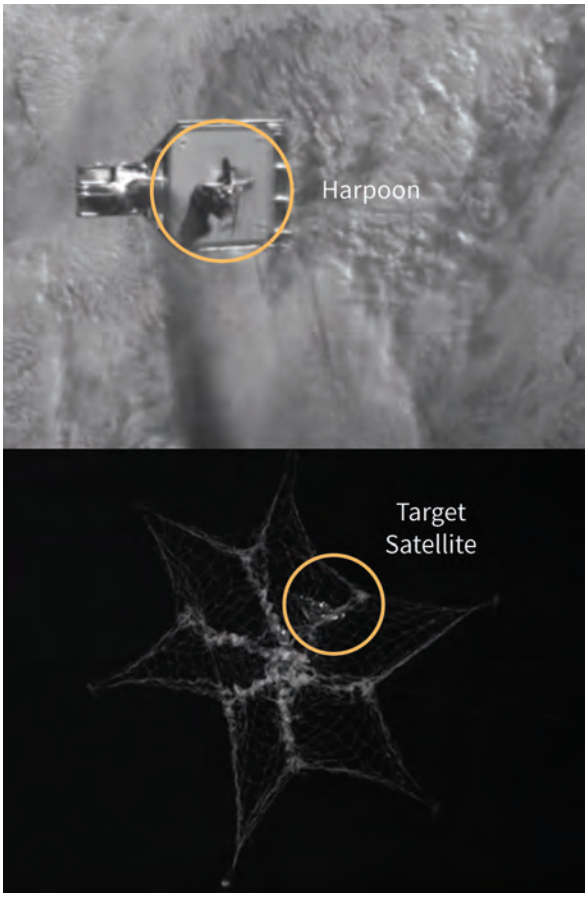


Figure 6: Orbital space launches from all countries (1957–2018).
SPACE-TRACK.ORG / CSIS AEROSPACE SECURITY[319]



Active debris removal in low Earth orbit. A research group at University of Surrey has demonstrated two techniques for removing space debris on-orbit: one using a harpoon (top) and another using a webbed net (bottom).
UNIVERSITY OF SURREY / BBC

Active Debris Removal

ACTIVE DEBRIS REMOVAL technology toes the line between the peaceful use of outer space and potential counterspace weapons. Almost any technology designed to move, de-orbit, or destroy an object in space could hypothetically be used against an adversary's satellite. However, space debris removal is a potentially lucrative business and companies from the United States, Japan, and other nations are developing several methods for active debris removal.[322]

A project led by the University of Surrey and sponsored by the European Commission and other partners has completed two successful tests of active debris removal in space.[323] **The project, known as RemoveDEBRIS, first successfully used a net to capture a pre-designated target in September 2018.**[324] **Later, in February 2019, the RemoveDEBRIS mission deployed a harpoon to spear a tethered plate.**[325]

back to at least four Egyptian military installations near Cairo.[318]

EUROPE

THE EUROPEAN SPACE AGENCY (ESA) is responsible for some of the most prominent aspects of today's space infrastructure, including the PNT system Galileo and the earth-observation system Copernicus. Through its Ariane and Vega launch vehicle families, launched from the Guiana Space Centre in French Guiana, the ESA supported eight launches last year. The Guiana Space Center also hosted three Soyuz rocket launches in 2018.[320] About 16 billion euros have been earmarked for space in the 2021–2027 EU budget, representing a continued interest in joint capabilities.[321] While ESA is a collective European agency, many European countries have developed their own independent capabilities as well.

European space capabilities that could have counterspace implications have been demonstrated in several instances. For example, in 2000 a British microsatellite, SNAP, was launched in the same faring as a larger Chinese microsatellite, *Tsinghua*-1. Despite initial technical difficulties, SNAP successfully maneuvered within 2km of the *Tsinghua*-1.[326] This demonstrated the maneuverability necessary to accomplish both kinetic and non-kinetic physical attacks. In 2012, Iran reported that Iranian broadcasts on the European Hotbird satellite network were being jammed by British technicians in Bahrain.[327] In 2010, Sweden performed a series of RPOs and formation flying with two experimental satellites, dubbed Mango and Tango.[328] And in August 2018, NASA and ESA confirmed plans for a collaborative mission—part of the cooperative Asteroid Impact and Deflection Assessment—to demonstrate the capability to redirect an asteroid using the force of a kinetic impact.[329] Although this technology is intended to be used for entirely peaceful purposes, its testing and development

India's Polar Satellite Launch Vehicle on February 15, 2017. The PSLV, breaking the previous record of highest-number of satellites launched on a single vehicle. The previous record was held by Russia with 34 satellites.

XINHUA / STRINGER VIA GETTY IMAGES

could also inform the design of a kinetic physical counterspace weapon.

INDIA

IN JULY 1980, India became the seventh country to indigenously launch its own satellite, using its SLV-3 rocket.[330] While India does not currently have a formal national space policy, the Indian Space Research Organization (ISRO) does make two sector-specific policies available publicly on satellite communications and remote sensing.[331] Furthermore, India does not have an official military department focused on space. Instead, "India established an Integrated Space Cell, located in the Integrated Defense Headquarters, which is comprised of all three branches of India's armed forces."[332] Currently, India has two operational orbital launch vehicles, the Polar Satellite Launch Vehicle (PSLV) and the Geosynchronous Satellite Launch Vehicle (GSLV). With these two vehicles, India conducted seven launches in 2018, just a fraction of the 61 total Indian launches since 1980, from their Satish Dhawan Space Centre.[333]

India has not successfully demonstrated a direct-ascent ASAT capability. However, high-ranking government officials have claimed such capability through their *Agni*-V ICBM system.[334] India most recently successfully tested its *Agni*-V ICBM in December 2018 from a mobile launch system. According to news sources, the Indian Ministry of Defense reported that the test was successful and all objectives were met.[335] In 2010, the then-head of India's Defense Research and Development Organization, Director General V.K. Saraswat, stated that India had the building blocks and capability to create a direct-ascent ASAT weapon, even if the country did not openly test the technology. Saraswat also stated that India would "validate the anti-satellite capability on the ground through simulation."[336] While they have reiterated that they possess

ASAT capabilities, Indian officials claim to not want to weaponize space or create harmful debris in orbit from a test.[337] India also has several medium-range and ICBMs that could be used to deliver a nuclear weapon into orbit.[338]

A 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 focus.[339] In 2013, a new *Technology Perspective and Capability Roadmap* noted a focus on developments in electronic weapons, specifically miniaturization of EW as payloads on satellites.[340]

In its 2018 *Technology Perspective and Capability Roadmap*, India detailed investments in a two-phased Tactical High Energy Laser System. The second phase of this system is intended to "be capable of anti satellite role from ground & aerial platform."[341] This same document also shows investment in an Integrated EW System with requirements to "detect, monitor, locate and jam enemy cellular receivers and satellite communication receivers."[342] Another system, the Aerostat Based EW System, has the same requirement as the integrated system, as well as being able to "carry out jamming & spoofing of satellite based positioning systems."[343]

INDIAN OFFICIALS ALSO STATE THAT THEY DO NOT WANT TO WEAPONIZE SPACE OR CREATE HARMFUL DEBRIS IN ORBIT FROM A TEST.

ISRAEL

THE ISRAEL SPACE AGENCY (ISA) was established in 1983 as part of the Ministry of Science and Technology.[344] While the ISA continues to emphasize a broad civil space infrastructure, "a diverse scope of activities was established both for defense led by Israel MOD and for civilian applications under the leadership of ISA."[345] Despite having a longstanding space agency, Israel lacks a clear national space policy.

On February 21, 2019, SpaceX successfully launched an Israeli startup company's lunar spacecraft named *Beresheet*, which in Hebrew means 'genesis.'[346] This is the nation's first lunar spacecraft, making Israel the fourth nation—behind Russia, the United States, and China—to land on the moon.[347] *Beresheet* was developed by an Israeli private commercial space company, SpaceIL. SpaceIL was created in 2011 to compete in Google's Lunar XPrize program, which ended without a winner. Despite this, SpaceIL continued developing *Beresheet* and launched it as a secondary payload on a Falcon 9 mission.[348]

In terms of counterspace capabilities, Israel's Arrow missile defense system could in theory be used as an ASAT weapon. Israel successfully demonstrated the required capabilities for an ASAT intercept (detection, targeting, and discrimination of a satellite target) using its Arrow 3 defense systems in December 2015.[349] Israel completed another successful test on January 22, 2019 of the same system.[350] Though not a true ASAT test, like that of China in 2007, the test proved that Israel could have a latent ASAT capability to hit satellites in LEO.

JAPAN

JAPAN HAS INCREASED its focus on developing space technologies since the Basic Space Law was passed in 2008.[351] In its recent National Defense Program Guidelines for FY 2019 and beyond, Japan states its plans to "ensure superiority in use of space at all stages from peacetime to armed contingencies" and to "work to strengthen capabilities including mission assurance capability and capability to disrupt opponent's command, control, communications and information."[352] To achieve these goals, Japan will leverage its national space enterprise, including the Self-Defense Forces, the Japan Aerospace Exploration Agency (JAXA), its growing defense-industrial base, and its longstanding relationship with the United States.

Due to the dual-use nature of many space technologies, even benign space capabilities can be viewed by others as counterspace weapons. In 1998, Japan proved it could rendezvous and successfully dock two orbiting satellites. In this same rendezvous, Japan tested the functionality of a robotic arm that could grapple and exercise coordinated control over a second satellite.[353] Both of these capabilities could be used as part of a co-orbital ASAT

weapon, but Japan has given no indication that it plans to do so.

LIBYA

THURAYA SATELLITE COMMUNICATIONS, a company based in the United Arab Emirates, accused Libyan nationals of multiple satellite jamming activities occurring over six months in 2006. Concerned that smugglers were using the company's services to bring illegal contraband into the country, Thuraya claimed that three separate locations in Libya carried out a barrage of jamming activities on its satellite communications services. The situation was rectified by "a diplomatic initiative made by the government of the United Arab Emirates to the government of Libya."[354] Five years later, in 2011, Thuraya's satellite communications were once again jammed over Libya.[355]

In February 2011, the UAE Telecommunications Regulatory Authority announced that several transmissions from two television broadcasting satellites were reportedly disrupted by frequent jamming.[356] According to press reports, the stations affected included: Five, BBC World, CNN International, US sports channels, other cable TV networks, and nearly two dozen radio stations. It was also reported that FBI communications were disrupted by the jamming.[357] Later that month, Al Jazeera also accused the Libyan government of jamming its satellite transmissions in the region. Al Jazeera reported that it had pinpointed the source of the jamming to a Libyan intelligence services building south of Tripoli.[358] It is unknown, whether these capabilities are still accessible by the Libyan Naitonal Army.

PAKISTAN

PAKISTAN IS INVESTING MORE in its space agency, the Space and Upper Atmosphere Research Organisation's (SUPARCO). SUPARCO's budget for fiscal year 2019 was reported to be 4.7 billion Pakistani rupees, or just under 34 million dollars. This includes allocations for the Pakistan Multi-Mission Satellite (PakSat-MM1), a Pakistan Space Centre in Karachi, Lahore, and Islamabad, as well as the establishment of Space Application Research Centre in Karachi.[359] Pakistan also plans on sending a human to space, with the help of China, by 2022.[360]

Pakistan has developed nuclear weapons and integrated them with ballistic missile systems. Pakistan's longest-range missile, the *Shaheen* 3, could potentially deliver a nuclear weapon into LEO.[361] However, Pakistan has not indicated that it plans to test or field a nuclear ASAT system.

UKRAINE

ELECTRONIC WARFARE HAS BEEN a staple of Russian activity in Ukraine, and the Ukrainian government is employing similar techniques to jam broadcasts supporting Moscow-backed separatists. In 2014, Ukraine attempted to jam Russian communications satellites that were broadcasting Russian television in the country.[362] Furthermore, Ukraine's secretary of the National Security and Defence Council has stated that "blocking the destructive influence of separatist and Russian information propaganda ... is one of our priorities."[363]

NON-STATE ACTORS

IN WHAT WAS POSSIBLY THE FIRST instance of satellite spoofing by a non-state actor, a disgruntled employee at a local satellite uplink station spoofed HBO programming in 1986 in order to display his own message: "Good evening, HBO, from Captain Midnight. $12.95 a month? No way! Showtime/The Movie Channel, beware."[364] Similarly, a Chinese spiritual organization, Falun Gong, spoofed Chinese satellite television broadcasts in 2002, replacing the footage with its own video.[365]

In 2007, the Tamil Tigers, a non-state actor based in Southeast Asia, hijacked an Intelsat satellite and replaced the feed with its own propaganda and data.[366] The attack caused Intelsat to shut down

the satellite transponder after more than a year of unauthorized use.[367]

In March 2011, after successful jamming operations by the Libyan government on communications satellites operated by the UAE-based company Thuraya, a team of rebels assisted by Libyan-American telecom executives were able to re-establish their own satellite communications. The March 2011 "cutoff had rebels waving flags to communicate on the battlefield." Several steps were taken to re-establish satellite telephone communications, including securing a direct feed to the jammed satellite to bypass the interference.[368]

Terrorist and insurgent organizations have also used electronic attacks against U.S. military space capabilities. In the early years of Operation Iraqi Freedom, insurgents or remnants of the former Iraqi regime repeatedly jammed commercial SATCOM links used by the U.S. military. At least five jamming instances were later determined to be deliberate jamming of the satellite uplink using a "sweeper" signal meant to create interference across a broad segment of the spectrum.[369] *The Washington Post*, in 2013, reported on concerns within the DIA that "al-Qaeda was sponsoring simultaneous research projects to develop jammers to interfere with GPS signals and infrared tags that drone operators rely on to pinpoint missile targets." The story cites an instance in 2011 in which U.S. intelligence believed that jihadists in Pakistan had started testing a GPS jamming capability for the first time.[370]

In 2014, a 25-year old British citizen was arrested for hacking into an unnamed satellite system used by the U.S. military, where he accessed hundreds of Pentagon employees' personal information. In the same attack, the hacker also accessed data from about 30,000 satellite phones.[371]

At the 2015 Chaos Communication Camp hacker conference, attendees were given "software-defined radios" sensitive enough to pick up on satellite traffic from Iridium communications satellites. A presentation entitled "Iridium Hacking: 'please don't sue us'" taught attendees just how easy it was to access Iridium communication links and eavesdrop on traffic.[372]

Sophisticated Truck Robbers

MEXICAN GANGS are conducting sophisticated highway robberies using small jammers—some of which can be powered by a cigarette lighter in a car. Armed robbers use these small jammers to target GPS downlinks to the truck's navigation system. These navigation systems are used to send the truck's location to the parent company or client in the case of an unplanned stop. Without this safety feature, police are typically not alerted of the robbery until after the crime has occured.[373]

WHAT TO WATCH

AS THIS REPORT DEMONSTRATES, many countries have developed and tested a variety of counterspace weapons. However, only a portion of the threats to space systems identified in this report make significant advances in any given year. This section details a shortlist of specific threats and technical developments that are important to watch in the near future.

For spacefaring nations with a history of successful kinetic physical ASAT tests, like China and Russia, an important area to watch is the development and testing of new boost systems that may suggest further diversification of kinetic physical counterspace threats. With ASAT tests every year for the past five years, it is likely China will continue to test and refine its direct-ascent ASAT capabilities. It would be unexpected, however, for China to conduct another ASAT test that creates debris, like its SC-19 test in 2007. For Russia, a key area to watch is evidence of tests relating to its air-launched and mobile ground-launched ASAT weapons. Unlike ASAT weapons that are launched from a spaceport, air-launched ASATs (like those launched from a MiG-31 fighter jet) and mobile ground-launched ASATs (like the PL-19/*Nudol*) could be deployed on short notice in the event of a crisis and are more difficult to track and neutralize.

Recent satellite imagery of launch sites in both Iran and North Korea suggest a renewed interest in orbital space launch capabilities. A successful orbital launch from either country would certainly be newsworthy, since Iran and North Korea have not placed an object in orbit since 2015 and 2016, respectively. Watch for new satellite imagery or public remarks suggesting renewed development of space launch infrastructure at the Imam Khomeini Space Center in Iran and the Sohae Satellite Launching Station in North Korea. For both countries, having a reliable space launch capability is a key precursor to developing kinetic physical counterspace weapons such as direct-ascent or co-orbital ASATs.

SATELLITES PERFORMING CLOSE APPROACHES OR RENDEZVOUS IN ANY ORBITAL REGIME COULD SUPPORT A BROAD RANGE OF COUNTERSPACE WEAPONS INCLUDING KINETIC PHYSICAL, NON-KINETIC PHYSICAL, AND ELECTRONIC.

China and Russia are also likely to continue the development and testing of RPO capabilities in both LEO and GEO. More specifically, a key activity to watch is the behavior of Chinese GEO satellite SJ-17 as it continues to perform rendezvous activities on orbit. So far, only other Chinese satellites have appeared to serve as targets for SJ-17's RPO activity. If the Chinese satellite approached other non-Chinese objects on orbit, those objects' operators might choose to make a public statement condemning the behavior, like the operators of satellites that have been approached by Russian GEO satellite *Olymp-K*. While *Olymp-K* has not caused international alarm since its close approach to a French-Italian military satellite in October 2017, it appears to have continued its RPO activities in the GEO belt since then. Satellites performing close approaches or rendezvous in any orbital regime could support a broad range of counterspace weapons including kinetic physical, non-kinetic physical, and electronic. A reckless close approach or malfunction in one of these satellites could result in a close call, potentially forcing an unplanned maneuver in one of the targeted satellites—or worse yet, a debris-producing collision in GEO.

Given the proliferation and ongoing use of electronic forms of attack against space systems, it is likely that the coming years will bring continued use of these counterspace weapons in both regional conflicts and pre-conflict situations. For example, both Russia and North Korea may continue to use electronic counterspace weapons in an attempt to disrupt or signal resolve in response to U.S.-allied military exercises that occur on their periphery. Another area to watch is the continued proliferation of these electronic forms of attack to other regional conflicts and new, possibly non-state, actors.

A final area, and perhaps the most important area to watch, is how the United States responds to new and ongoing developments in the counterspace capabilities of others. The 2018 National Defense Strategy says the military will prioritize "resilience, reconstitution, and operations" to protect space assets. What remains to be fully defined, however, are the specific steps the Department of Defense intends to take to improve the protection of space systems across the full spectrum of threats posed by potential adversaries. Key developments to watch within the United States are changes in the organization of the national security space enterprise, further development and articulation of military space strategy and doctrine, and investments in new space capabilities, counterspace capabilities, and space situational awareness capabilities. Changes in these areas are an indication of the level of priority being placed on space and how the United States intends to compete in this domain.

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 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. 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 a research associate and program manager of the CSIS Aerospace Security Project. His research interests include satellite system architecture analysis, civil and commercial space operations, and international collaboration in science research. 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 is the host and executive producer of *Moonstruck*, a podcast about the history of human spaceflight. He 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.

MADISON BERGETHON is a research intern for the CSIS Aerospace Security Project. Prior to joining CSIS, Madison worked for the government affairs and international business team at SpaceX. She is a senior at The George Washington University studying international affairs and naval science. As a designated student naval aviator she will attend flight school in the summer of 2019, after commissioning as an officer in the United States Navy.

ALEXANDRA COULTRUP is a research intern for the CSIS Aerospace Security Project. She is a graduate student at Florida Institute of Technology, pursuing an MS in aviation human factors with a concentration in spaceflight safety. Prior to joining CSIS, Ms. Coultrup worked at local NPR station WFIT 89.5 FM and Thales Avionics. Ms. Coultrup also serves as a graduate research assistant at the Aldrin Space Institute at Florida Tech.

APPENDIX I

LIST OF ACRONYMS USED

AEHF	Advanced Extremely High Frequency
ASAT	Anti-Satellite
BBC	British Broadcasting Corporation
BMD	Ballistic Missile Defense
CASC	China Aerospace Science and Technology Corporation
CHEOS	China High-resolution Earth Observation System
CNAS	China National Space Administration
DIA	Defense Intelligence Agency
DoD	U.S. Department of Defense
EMP	Electromagnetic Pulse
ESA	European Space Agency
EW	Electronic Warfare
GBS	Global Broadcast Service
GEO	Geosynchronous Orbit
GLONASS	Global Navigation Satellite System (Russia)
GPS	Global Positioning System
GSLV	Geosynchronous Satellite Launch Vehicle
HPM	High Powered Microwave
ICBM	Intercontinental Ballistic Missile
ILRS	International Laser Ranging Service
IS	Istrebitel Sputnikov (Russia)
ISA	Israel Space Agency
ISR	Intelligence, Surveillance, and Reconnaissance
ISS	International Space Station
JAXA	Japan Aerospace Exploration Agency
JCPOA	Joint Comprehensive Plan of Action
KCNA	Korean Central News Agency (North Korea)
LEO	Low Earth Orbit
MEO	Medium Earth Orbit
MMW	Millimeter Wave
MRBM	Medium-Range Ballistic Missiles
NADA	National Aerospace Development Administration (North Korea)
NASA	National Aeronautics and Space Administration
NOAA	National Oceanographic and Atmospheric Administration
NRO	U.S. National Reconnaissance Office
PKK	Kurdistan Workers' Party
PLA	People's Liberation Army (China)
PNT	Positioning, Navigation, and Timing

PSLV	Polar Satellite Launch Vehicle (India)
RF	Radio Frequency
RPO	Rendezvous and Proximity Operations
SASTIND	State Administration for Science, Technology, and Industry for National Defense
SATCOM	Satellite Communications
SLV	Satellite Launch Vehicle (India)
SSF	Strategic Support Force (China)
SUPARCO	Space and Upper Atmosphere Research Organisation
S&T	Science and Technology
TEL	Transporter erector-launcher
UHF	Ultra High Frequency
VOA	Voice of America
WGS	Widespread Global SATCOM (Satellite Communications)

ENDNOTES

INTRODUCTION

1 U.S. Department of Defense, *Summary of the National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: U.S. Department of Defense, 2018), 3, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

2 Robert Bowman, *Star Wars: A Defense Insider's Case Against the Strategic Defense Initiative* (Los Angeles: Tarcher Publications, 1986), 14.

TYPES OF COUNTERSPACE WEAPONS

3 Michael R. Pence, "Remarks by Vice President Pence on the Future of the U.S. Military in Space" (speech, The Pentagon, Arlington, VA, August 9, 2018), https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-future-u-s-military-space/.

4 Ibid.

5 U.S. Congress, 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.

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

7 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.

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

9 Garino and Gibson, "Space System Threats," 274.

10 Qualitative Reasoning Group at Northwestern University, "Communications System," http://www.qrg.northwestern.edu/projects/vss/docs/communications/1-what-are-uplink-and-downlink.html.

11 Garino and Gibson, "Space System Threats," 274.

12 Ibid., 275.

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

14 Richard B. Langley, Mark L. Psiaki, Steven P. Powell, and Brady W. O'Hanlon. "Innovation: GNSS Spoofing Detection," *GPS World*, June 1, 2013, http://gpsworld.com/innovation-gnss-spoofing-detection-correlating-carrier-phase-with-rapid-antenna-motion/.

15 The University of Texas at Austin, "UT Austin Researchers Successfully Spoof an $80 Million Yacht at Sea," UT News, July 29, 2013,https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/.

16 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

17 Thomas G. Roberts, *Spaceports of the World* (Washington D.C.: Center for Strategic and International Studies, March 13, 2019), https://aerospace.csis.org/spaceports-of-the-world/.

18 Zhenglimin,"Backgrounder: Xi Jinping's Vision for China's Space Development," CCTV News, April 24, 2017, http://english.cctv.com/2017/04/24/ARTIZBj8dd7ULWfpwuw8nJp5170424.shtml.

19 Roberts, *Spaceports of the World*.

20 Andrew Jones, "China Will Attempt 30-plus Launches in 2019, including Crucial Long March 5 Missions," SpaceNews, January 29, 2019, https://spacenews.com/china-will-attempt-30-plus-launches-in-2019-including-crucial-long-march-5-missions/.

21 Li Xia, "China's Long March-5 Rocket to Resume Flight in July," Xinhua News Agency, January 29, 2019, http://www.xinhuanet.com/english/2019-01/29/c_137784351.htm.

22 CSIS Aerospace Security, "Space Environment: Total Launches by Country," Center for Strategic and International Studies, accessed April 4, 2019, https://aerospace.csis.org/data/space-environment-total-launches/.

23 Andrew Jones, "Chang'e-4 powers down for second lunar night," SpaceNews, February 11, 2019, https://spacenews.com/change-4-powers-down-for-second-lunar-night/.

24 ChinaPower,"What's driving China's race to build a space station?," Center for Strategic and International Studies, December 7, 2016, https://chinapower.csis.org/chinese-space-station/.

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

26 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.

27 Joan Johnson-Freese, "China Launched More Rockets into Orbit in 2018 than Any Other Country," *MIT Technology Review*, December 19, 2018, https://www.technologyreview.com/s/612595/china-launched-more-rockets-into-orbit-in-2018-than-any-other-country/.

28 Bryce Space and Technology, LLC, "Global Space Industry Dynamics," (Alexandria, VA: Bryce Space and Technology, 2017), 3, https://bryce

tech.com/downloads/Global_Space_Industry_Dynamics_2017.pdf.

29 Office of the Secretary of Defense, "Annual Report to Congress: Military Power of the People's Republic of China 2018," U.S. Department of Defense, May 16, 2018, 1, https://media.defense.gov/2018/Aug/16/2001955282/-1/-1/1/2018-CHINA-MILITARY-POWER-REPORT.PDF#page=14.

30 Space Angels, "Q4 2018," *Space Investment Quarterly*, October 9, 2018, 3, https://spaceangels.docsend.com/view/z6s9ugb.

31 Ibid., 11.

32 Bryce Space and Technology, LLC, "Start-Up Space: Update on Investment in Commercial Space Ventures" (Alexandria, VA: Bryce Space and Technology, 2018), v, https://brycetech.com/downloads/Bryce_Start_Up_Space_2018.pdf.

33 Andrew Jones, "Chinese Rocket Maker OneSpace Secures $44m in Funding; Expace Prepares for Commercial Launch," SpaceNews, August 14, 2018, https://spacenews.com/chinese-rocket-maker-onespace-secures-44m-in-funding-expace-prepare-for-commercial-launch/.

34 Andrew Jones, "Chinese Companies OneSpace and iSpace Are Preparing for First Orbital Launches," SpaceNews, January 24, 2019, https://spacenews.com/chinese-companies-onespace-and-ispace-are-preparing-for-first-orbital-launches/.

35 Stephen Clark, "LandSpace Falls Short of Orbit in Private Chinese Launch Attempt," Spaceflight Now, October 28, 2018, https://spaceflightnow.com/2018/10/28/landspace-falls-short-of-orbit-in-private-chinese-launch-attempt/.

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), 8, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2058/RAND_RR2058.pdf.

37 Andrew Jones, "China Completes 22nd Launch This Year with Gaofen-11, Matches National Record," SpaceNews, July 31, 2018, https://spacenews.com/china-completes-22nd-launch-this-year-with-gaofen-11-matches-national-record/.

38 Mike Wall, "China Launches Pioneering 'Hack-Proof' Quantum-Communications Satellite," Space.com, August 16, 2016, https://www.space.com/33760-china-launches-quantum-communications-satellite.html.

39 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.

40 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.

41 Pollpeter, Chase, and Heginbotham, "The Creation of the PLA Strategic Support Force," 3–4.

42 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/Hearing%20Transcript%20-%20February%2015%2C%202018.pdf.

43 Pollpeter, Chase, and Heginbotham, "The Creation of the PLA Strategic Support Force," 7.

44 U.S. Defense Intelligence Agency, "China Military Power: Modernizing a Force to Fight and Win," (Washington, DC: U.S. Defense Intelligence Agency, 2018), 97, http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/China_Military_Power_FINAL_5MB_20190103.pdf.

45 Office of the Secretary of Defense, "Annual Report to Congress," 14.

46 U.S. Defense Intelligence Agency, "China Military Power," 40.

47 Pollpeter, Chase, and Heginbotham, "The Creation of the PLA Strategic Support Force," 7.

48 Ibid.

49 United Nations Office of Outer Space Affairs, "Office for Outer Space Affairs and China Renew Commitment to Cooperation in Space Activities," April 21, 2017, http://www.unoosa.org/oosa/en/informationfor/media/2017-unis-os-479.html.

50 People's Liberation Army National Defense University,"China Military Encyclopedia, Second Edition" (Beijing, PRC: Encyclopedia of China Publishing House, 2007), 211, quoted in Bruce W. MacDonald, et al., "Crisis Stability in Space," 29.

51 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), 283-284, https://www.uscc.gov/sites/default/files/Annual_Report/Chapters/Chapter%202%2C%20Section%202%20-%20China%27s%20Space%20and%20Counterspace%20Programs.pdf.

52 The State Council Information Office of the People's Republic of China, "China's Military Strategy."

53 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.

54 Colin Clark, "Chinese ASAT Test Was 'Successful:' Lt. Gen. Raymond," Breaking Defense, April 14, 2015, https://breakingdefense.com/2015/04/chinese-asat-test-was-successful-lt-gen-raymond/.

55 Weeden and Samson, eds., *Global Counterspace Capabilities*, 1–11.

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

57 U.S. Defense Intelligence Agency, "China Military Power," 43.

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

59 Weeden and Samson, eds., *Global Counterspace Capabilities*, 1–12.

60 "China Again Conducts a High Altitude Science Mission: Higher Altitude and More Data" (中国再次高空科学探测试验：高度更高数据更多), China News (中国新闻网), May 14, 2013,http://www.chinanews.com/gn/2013/05-14/4817925.shtml.

61 Weeden and Samson, eds., *Global Counterspace Capabilities*, 1–14.

62 U.S.-China Economic and Security Review Commission, "2015 Report to Congress," 293.

63 U.S. Congress, Senate, Select Committee on Intelligence, *Worldwide Threat Assessment of the US Intelligence Community, written statement of Daniel R. Coats*, January 29, 2019, 17, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

64 Mike Gruss, "U.S. State Department: China Tested Anti-satellite Weapon," SpaceNews, July 28, 2014, https://spacenews.com/41413us-state-department-china-tested-anti-satellite-weapon/.

65 Mike Gruss, "Senior U.S. Official Insists China Tested ASAT Weapon," SpaceNews, August 25, 2014, https://spacenews.com/41676senior-us-official-insists-china-tested-asat-weapon/.

66 Weeden and Samson, eds., *Global Counterspace Capabilities*, 1–16.

67 Bill Gertz, "China ASAT Test Part of Growing Space War Threat," The Washington Free Beacon, February 23, 2018, http://freebeacon.com/national-security/asat-test-highlights-chinas-growing-space-warfare-capabilities/.

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

69 Weeden and Samson, eds., *Global Counterspace Capabilities*, 1–11.

70 U.S. Defense Intelligence Agency, "China Military Power," 41.

71 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.

72 Ibid.

73 Weeden and Samson, eds., *Global Counterspace Capabilities*, 1–2.

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

75 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.

76 Pollpeter, Chase, and Heginbotham, "The Creation of the PLA Strategic Support Force," 10.

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

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

79 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/.

80 "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.

81 "SJ 17," Gunter's Space Page, 2019, https://space.skyrocket.de/doc_sdat/sj-17.htm.

82 "In-Space Eavesdropping? – China's Shijian-17 Completes High-Altitude Link-Up," Spaceflight 101, December 9, 2016, http://spaceflight101.com/cz-5-maiden-flight/shijian-17-rendezvous-with-chinasat-5a/.

83 Colin Clark, "China Satellite SJ-17, Friendly Wanderer?" Breaking Defense, April 19, 2018, https://breakingdefense.com/2018/04/china-satellite-sj-17-friendly-wanderer/.

84 International Institute for Strategic Studies, *The Military Balance 2017* (London: Routledge, 2017), 19–26.

85 *Worldwide Threat Assessment of the US Intelligence Community*, Daniel R. Coats, 2018, 13.

86 U.S. Defense Intelligence Agency, "Challenges to Security in Space," (Washington, DC: U.S. Defense Intelligence Agency, February 11, 2019), 20, http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.

87 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.

88 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, 6, https://www.uscc.gov/sites/default/files/Fisher_Combined.pdf.

89 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/.

90 Francis Harris, "Beijing secretly fires lasers to disable US satellites," *Telegraph*, September 26, 2006, https://www.telegraph.co.uk/news/worldnews/1529864/Beijing-secretly-fires-lasers-to-disable-US-satellites.html.

91 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.

92 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.

93 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.

94 Fisher, Jr., "China's Progress with Directed Energy Weapons," 9.

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

96 Office of the Secretary of Defense, "Annual Report to Congress," 74.

97 Ibid., 21.

98 U.S.-China Economic and Security Review Commission, "2015 Report to Congress," 297–298.

99 U.S. Defense Intelligence Agency, "Challenges to Security in Space," 20.

100 Lin Jin-shun, Wu Xianzhong, Lu Shengjun, and Jiang Chunshan, "Countermeasure Technology for MMW Satellite Links," *Aerospace Electronic Warfare*, October 2012, 20–22, as quoted in David D. Chen, "Opening Statement of Mr. David Chen," 82.

101 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/.

102 Huang Lin and Yang Qing, "GPS Spoofing: Low-cost GPS Simulator" (presentation, 23rd Annual DefCon, Las Vegas, NV, August 6-9, 2015), https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/DEFCON-23-Lin-Huang-Qing-Yang-GPS-Spoofing.pdf

103 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.

104 "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.

105 Stephen Chen, "Could China Be Trying to Play God with the Weather?" *South China Morning Post*, June 2, 2018, https://www.scmp.com/news/china/society/article/2148697/could-new-chinese-radar-system-really-be-used-play-god-weather.

106 Ibid.

107 Nick Whigham, "A new Chinese radar facility could become a weapon hiding in plain sight," News.com.au, August 26, 2018, https://www.news.com.au/technology/science/space/a-new-chinese-radar-facility-could-become-a-weapon-hiding-in-plain-sight/news-story/acbe423f03b2e1d042723892bb080bb8.

108 Office of the Secretary of Defense, "Annual Report to Congress," 40.

109 The State Council Information Office of the People's Republic of China, "China's Military Strategy."

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

111 U.S. Defense Intelligence Agency, "China Military Power," 46.

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

113 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.

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

115 Ibid.

116 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.

117 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.

118 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/.

119 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-idUSKCN1PO1AN.

RUSSIA

120 Roberts, *Spaceports of the World*.

121 U.S. Department of Defense, *Missile Defense Review* (Washington, DC: U.S. Department of Defense, 2019) VI, https://media.defense.gov/2019/Jan/17/2002080666/-1/-1/1/2019-MISSILE-DEFENSE-REVIEW.PDF.

122 Todd Harrison et al., *Escalation and Deterrence in the Second Space Age*, (Washington DC: Center for Strategic and International Studies, October 3, 2017), https://aerospace.csis.org/escalation-deterrence-second-space-age/.

123 Roberts, *Spaceports of the World*.

124 Ibid.

125 Ibid.

126 Todd Harrison and Nahmyo Thomas, "NASA in the Second Space Age: Exploration, Partnering, and Security," *Strategic Studies Quarterly*, Winter 2016, 3, http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-10_Issue-4/Harrison.pdf; "Partners Sign ISS Agreements," NASA, October 23, 2010, https://www.nasa.gov/mission_pages/station/structure/elements/partners_agreement.html.

127 Thomas G. Roberts, "Beyond the Glass Ceiling: Why NASA Must Continue to Launch a Diverse Astronaut Corps," CSIS Aerospace Security, July 31, 2018, https://aerospace.csis.org/beyond-the-glass-ceiling-why-nasa-must-continue-to-launch-a-diverse-astronaut-corps/.

128 Sarah Lewin, "Russians ID Cause of Soyuz Launch Abort, Release Dramatic Rocket Video," Space.com, November 1, 2018, https://www.space.com/42319-soyuz-launch-abort-russia-identifies-cause.html; Thomas G. Roberts, "International Astronaut Database," CSIS Aerospace Security, December 3, 2018, https://aerospace.csis.org/data/international-astronaut-database/.

129 Anatoly Zak, "Russian space program in the 2010s: decadal review," Russian Space Web, February 11, 2019, http://www.russianspaceweb.com/russia_2010s.html#2019.

130 Ibid.

131 CSIS Aerospace Security, "Space Environment."

132 Yuri Urlichich et al., "GLONASS Modernization," *GPS World*, November 1, 2011, http://gpsworld.com/glonass-modernization-12232/.

133 «На противника посмотрят с двухметровой объективностью,» *Коммерсантъ*, July 28, 2018, https://www.kommersant.ru/doc/3049019; «The ExoMars Programme 2016-2020,» European Space Agency, http://exploration.esa.int/mars/46048-programme-overview/; Asif Siddiqi, «Russia Is the Only Nation That Regularly Sends Humans to Orbit, But Its Space Program Is in Trouble,» *Slate Magazine*, March 21, 2017, http://www.slate.com/articles/technology/future_tense/2017/03/russia_s_space_program_is_in_trouble.html.

134 Paulina Glass, "Russia Is Slowly Declining As a Space Superpower," Defense One, August 5, 2018, https://www.defenseone.com/threats/2018/08/russia-slowly-declining-space-superpower/150279/.

135 Elizabeth Howell, "Roscosmos: Russia's Space Agency," Space.com, January 29, 2018, https://www.space.com/22724-roscosmos.html; "Roscosmos General Information," Roscosmos, undated, accessed February 7, 2019, http://en.roscosmos.ru/119/.

136 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/.

137 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/.

138 Ministry of Defence of the Russian Federation, "Aerospace Defence Forces," Russian Federation, undated, accessed February 7, 2019, http://eng.mil.ru/en/structure/forces/cosmic.htm.

139 President of the Russian Federation, "The Military Doctrine of the Russian Federation," December 2014, https://rusemb.org.uk/press/2029.

140 Ibid.

141 Nuclear Threat Initiative, "Proposed Prevention of an Arms Race in Space (PAROS) Treaty," Nuclear Threat Initiative, September 29, 2017, http://www.nti.org/learn/treaties-and-regimes/proposed-prevention-arms-race-space-paros-treaty/.

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

143 Alexander Velez-Green, *The Unsettling View from Moscow: Russia's Strategic Debate on a Doctrine of Pre-emption* (Washington, DC, Center for a New American Security), April 27, 2017, 11, https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-RussiaStrike-Finalb.pdf.

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

145 U.S. Defense Intelligence Agency, "Russia Military Power: Building a Military to Support Great Power Aspirations" (Washington, DC: Defense Intelligence Agency, 2017), 36, http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf?ver=2017-06-28-144235-937; "Рогозин не исключил, что американский космоплан X-37 может нести оружие," TASS, October 1, 2018, https://tass.ru/kosmos/5625023.

146 "US creating pretexts for militarization of space — Russian General Staff," TASS, March 3, 2018, http://tass.com/defense/1047214.

147 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

148 "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.

149 Ibid., 3.

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

151 Ankit Panda, "Russia Conducts New Test of 'Nudol' Anti-Satellite System," *Diplomat*, April 2, 2018, https://thediplomat.com/2018/04/russia-conducts-new-test-of-nudol-anti-satellite-system/; Bill Gertz, "Russia Flight Tests Anti-Satellite Missile."

152 "Russian S-300 missile systems capable of targeting near space 'enter service'," *RT International*, March 12, 2015, https://www.rt.com/news/239961-near-space-missile-defense/; Missile Defense Project, "S-300," CSIS Missile Threat, July 13, 2018, https://missilethreat.csis.org/defsys/s-400/; Missile Defense Project, "S-400 Triumf," CSIS Missile Threat, June 15, 2018, https://missilethreat.csis.org/defsys/s-400-trumf/.

153 Vladimir Karnozov, "Russia's Next-generation S-500 SAM Enters Production," AIN Online, March 14, 2018, https://www.ainonline.com/aviation-news/defense/2018-03-14/russias-next-generation-s-500-sam-enters-production.

154 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.

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

156 Steve Lambakis, "Foreign Space Capabilities: Implications for U.S. National Security," National Institute for Public Policy (Fairfax, VA: National Institute Press, 2017), http://www.nipp.org/wp-content/uploads/2017/09/Foreign-Space-Capabilities-pub-2017.pdf; Missile Defense Project, "Russia Tests S-500 Air Defense System" CSIS Missile Threat, September 28, 2017, https://missilethreat.csis.org/russia-successfully-tests-s-500-air-defense-system/.

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

158 "Mikoyan-Gurevich MiG-31BM Foxhound," JetPhotos, September 14, 2018, https://www.jetphotos.com/photo/9074544.

159 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.

160 U.S. Congress, Senate, Committee on Armed Services, *Worldwide Threat Assessment of the US Intelligence Community*, written statement of James Clapper, February 9, 2016, 10, https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf.

161 Alexander Zudin, “Russia to Deploy Anti-satellite Weapon on MiG-31BM,” *IHS Jane’s Missiles and Rockets*, February 22, 2017.

162 Jana Honkova, The Russian Federation’s Approach to Military Space and Its Military Space Capabilities (Arlington, VA: George C. Marshall Institute, 2013); “Эксперт: разрабатываемая в РФ противоспутниковая ракета эффективнее существующих в мире,” TASS, October 26, 2018, https://tass.ru/armiya-i-opk/5725426.

163 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.

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

165 Ibid.

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

167 “Briz,” Gunter’s Space Page, 2019, http://space.skyrocket.de/doc_stage/briz.htm.

168 “Okno ELINT complex in Tajikistan is becoming Russian,” *Ferghana News*, April 17, 2006, http://enews.fergananews.com/article.php?id=1390; Alexander Zolotukhin, “Space Force of Russia: Guarding the Space Borders of the State for Ten Years,” *News Line Novosti Kosmonavtiki*, July 3, 2011.

169 “«Окно» в Таджикистане «увидит» 50 тысяч км космоса,” *Rambler*, November 27, 2016, https://news.rambler.ru/science/35393642-okno-v-tadzhikistane-uvidit-50-tysyach-km-kosmosa/.

170 Bart Hendrickx, “Russia Develops Co-orbital Anti-satellite Capability,” *Jane’s Intelligence Review*, September 27, 2018, 1.

171 Ibid., 8.

172 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.

173 Jonathan McDowell, “Jonathan’s Space Report,” August 17, 2018, http://planet4589.org/space/jsr/back/news.752.txt.

174 Yleem D.S. Poblete, “Remarks on Recent Russian Space Activities of Concern” (speech, Conference on Disarmament, Geneva, Switzerland, August 14, 2018), https://www.state.gov/t/avc/rls/285128.htm.

175 Wall, “’Very Abnormal’ Russian Satellite Doesn’t Seems So Threatening, Experts Say”; Brian Weeden, Twitter post, August 16, 2018, 9:46 a.m., https://twitter.com/brianweeden/status/1030088386042679297.

176 Weeden and Samson, eds., *Global Counterspace Capabilities*, 2-2; Hendrickx, “Russia Develops Co-orbital Anti-satellite Capability,” 5.

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

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

179 Thomas G. Roberts, “Russian Rendezvous and Proximity Operations in the GEO Belt,” CSIS Aerospace Security Project, accessed April 4, 2019, www.aerospace.csis/olymp.

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

181 MIke Gruss, “Russian Satellite Maneuvers, Silence Worry Intelsat,” Space News, October 9, 2015, https://spacenews.com/russian-satellite-maneuvers-silence-worry-intelsat/.

182 Peter, “Russia Shrugs off US Anxiety over Military Satellite.”

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

184 Missile Defense Project, “Missiles of Russia,” CSIS Missile Threat, 2018, https://missilethreat.csis.org/country/russia/.

185 U.S. Congress, House, Committee on Homeland Security, Subcommittee on Oversight and Management Efficiency, *Empty Threat or Serious Danger: Assessing North Korea’s Risk to the Homeland*, written statement of William R. Graham and Peter Vincent Pry, 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,” FutureScience, http://www.futurescience.com/emp/test184.html.

186 Siddiqi, “The Soviet Co-Orbital Anti-Satellite System,” 230.

187 Clay Wilson, *High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments, Congressional Research Service*, July 21, 2008,https://fas.org/sgp/crs/natsec/RL32544.pdf ; Mark Schneider, “Emerging EMP Threat to the United States,” National Institute for Public Policy (Fairfax, VA: National Institute Press, 2007), http://www.nipp.org/wp-content/uploads/2014/12/EMP-Paper-Final-November07.pdf.

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

189 Ibid.

190 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.

191 Alexei Mikhailov, “Пиу-пиу,” Lenta.ru, May 22, 2013, https://lenta.ru/articles/2012/11/13/russianlaser/; “Beams away: Russia boosts air-

borne combat laser program," *Russia Today*, November 19, 2012, https://www.rt.com/op-ed/soviet-airborne-laser-restarted-600/.

192 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/.

193 «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.

194 Hendrickx, "Russia Develops Co-orbital Anti-satellite Capability", 9; Steven Aftergood, "The Okno and Krona Space Surveillance Systems," The Federation of American Scientists, January 31, 2008, https://fas.org/blogs/secrecy/2008/01/the_okno_and_krona_space_surve/.

195 «Космические войска получили лазерный локатор,» *Коммерсантъ*, May 25, 2018, 4, https://www.kommersant.ru/doc/581197.

196 National Aeronautics and Space Administration, "International Laser Ranging Service (ILRS)," November 14, 2017, https://ilrs.cddis.eosdis.nasa.gov/network/stations/index.html.

197 Weeden and Samson, eds., *Global Counterspace Capabilities*, 2–26.

198 "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.

199 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/; "Russian R-330Zh jammer detected 7 km from the contact line in Donbas," Inform Napalm, November 16, 2017, https://informnapalm.org/en/russian-r-330zh-jammer-detected-7-km-from-the-contact-line-in-donbas/.

200 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/.

201 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; David Stupples, "How Syria is becoming a test bed for high-tech weapons of electronic warfare," Conversation, October 8, 2015, https://theconversation.com/how-syria-is-becoming-a-test-bed-for-high-tech-weapons-of-electronic-warfare-48779.

202 Courtney Kube, "Russia Has Figured out How to Jam U.S. Drones in Syria, Officials Say," NBC News, April 10, 2018, https://www.nbcnews.com/news/military/russia-has-figured-out-how-jam-u-s-drones-syria-n863931.

203 "Russian Exercise Jams Aircraft GPS in North Norway for a Week," Resilient Navigation and Timing Foundation, October 5, 2017, https://rntfnd.org/2017/10/05/russian-exercise-jams-aircraft-gps-in-north-norway-for-a-week-nrk/.

204 Ibid.

205 Dave Johnson, "ZAPAD 2017 and Euro-Atlantic Security," NATO Review, December 14, 2017, https://www.nato.int/docu/review/2017/also-in-2017/zapad-2017-and-euro-atlantic-security-military-exercise-strategic-russia/en/index.htm.

206 North Atlantic Treaty Organization, "Trident Juncture 18," October 31, 2018, https://www.nato.int/cps/en/natohq/news_158620.htm.

207 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.

208 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.

209 Ibid.

210 "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/.

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.

212 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.

213 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; "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.

214 Damien McGuinness, "How a cyber attack transformed Estonia," BBC News, April 27, 2017, http://www.bbc.com/news/39655415.

215 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.

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

217 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.

IRAN

218 Roberts, *Spaceports of the World*.

219 *Worldwide Threat Assessment of the US Intelligence Community*, Daniel R. Coats, 2019, 10.

220 Aria Bendix, "Iran Claims It Launched a Satellite-Carrying Rocket Into Space," *Atlantic*, July 28, 2017, https://www.theatlantic.com/news/archive/2017/07/iran-claims-it-launched-a-satellite-carrying-rocket-into-space/535161/.

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

222 "Russia, Kazakhstan Sign Agreement on Creation of Baiterek Launch Complex at Baikonur," *Azernews*, August 22, 2018, https://www.azernews.az/region/136542.html.

223 "Safir," Gunter's Space Page, 2019, https://space.skyrocket.de/doc_lau/safir.htm; Thérèse Delpech, "Nuclear Deterrence in the 21st Century: Lessons from the Cold War for a New Era of Strategic Piracy" (Santa Monica, CA: RAND Corporation, 2012), 147, https://www.rand.org/pubs/monographs/MG1103.html.

224 Ali Akbar Dareini, "Iran's space monkey business: A plausible explanation?" *Christian Science Monitor*, February 4, 2013, https://www.csmonitor.com/Science/2013/0204/Iran-s-space-monkey-business-A-plausible-explanation.

225 Jeffrey Lewis, Twitter post, January 9, 2019, 2:20 p.m., https://twitter.com/ArmsControlWonk/status/1083126388121575426.

226 Stephen Clark, "Iran Admits Failure in Satellite Launch Attempt," January 16, 2019, https://spaceflightnow.com/2019/01/16/iran-admits-failure-in-satellite-launch-attempt/.

227 Note: The Simorgh launch vehicle is also known as the Safir-2; "Simorgh (Safir-2)," Gunter's Space Page, 2019, https://space.skyrocket.de/doc_lau/simorgh.htm; Missile Defense Project, "Simorgh," CSIS Missile Threat, Center for Strategic and International Studies, September 28, 2017, https://missilethreat.csis.org/missile/simorgh/.

228 *Worldwide Threat Assessment of the US Intelligence Community*, Daniel R. Coats, 2019, 10.

229 Jon Gambrell, "Images suggest Iran has attempted second satellite launch," *Times of Israel*, February 7, 2019, https://www.timesofisrael.com/images-suggest-iran-launched-satellite-despite-us-criticism/.

230 Carol Morello, "U.S. warns Iran against satellite launches it says could advance missile technology," *Washington Post*, January 3, 2019, https://www.washingtonpost.com/world/national-security/us-warns-iran-not-to-launch-satellites-into-space/2019/01/03/c4bba67c-0f6c-11e9-84fc-d58c33d6c8c7_story.html?.

231 Sarah Lewin, "Satellite Photos Show Evidence of Iranian Rocket Launch. But Did It Fail?," Space.com, February 7, 2019, https://www.space.com/43260-iran-second-satellite-launch-possible-failure.html.

232 Geoff Brumfiel, "Satellite Imagery Suggests 2nd Iranian Space Launch Has Failed," National Public Radio, February 6, 2019, https://www.npr.org/2019/02/06/692071812/satellite-imagery-suggests-second-iranian-space-launch-has-failed.

233 Jon Gambrell, "Images suggest Iran has attempted second satellite launch," *Washington Post*, February 7, 2019, https://www.washingtonpost.com/world/middle_east/images-suggest-iran-launched-2nd-satellite-over-us-criticism/2019/02/06/88e603fa-2a7d-11e9-906e-9d55b6451eb4_story.html?.

234 Brumfiel, "Satellite Imagery Suggests 2nd Iranian Space Launch Has Failed."

235 Mike Wall, "Iran claims to open space tracking center," Space.com, June 11, 2013, https://www.space.com/21521-iran-space-tracking-center.html.

236 William J. Broad and David E. Sanger, "Iran joins the space club, but why?" *New York Times*, April 4, 2006, http://www.nytimes.com/2006/04/04/science/space/04rock.html.

237 "Iranian Space Agency," Iran Watch, Wisconsin Project on Nuclear Arms Control, August 31, 2009, https://www.iranwatch.org/iranian-entities/iranian-space-agency.

238 "سازمان فضایی ایران،» Iranian Space Agency, July 9, 2016, https://www.isa.ir/find.php?item=1.66.10.fa.

239 Lambakis, "Foreign Space Capabilities: Implications for U.S. National Security," 31.

240 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.

241 "Gulf Security after 2020: Iran's Missile Priorities after the Nuclear Deal," International Institute for Strategic Studies, December 19, 2017, https://www.iiss.org/blogs/analysis/2017/12/gulf-security.

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

243 Missile Defense Project, "Safir," CSIS Missile Threat, October 16, 2017, https://missilethreat.csis.org/missile/safir/.

244 Max Fisher, "Deep in the Desert, Iran Quietly Advances missile Technology," *New York Times*, May 23, 2011, https://www.nytimes.com/2018/05/23/world/middleeast/iran-missiles.html.

245 Ibid.

246 Chase Winter, "Iran's military power: What you need to know," *DW*, August 6, 2018, https://www.dw.com/en/irans-military-power-what-you-need-to-know/a-43756843.

247 Missile Defense Project, "Missiles of Iran," CSIS Missile Threat, June 14, 2018, https://missilethreat.csis.org/country/iran/; National Coordination Office for Space-Based Positioning, Navigation, and Timing,"Control Segment," May 2017, accessed February 25, 2019, /www.gps.gov/multimedia/images/GPS-control-segment-map.pdf.

248 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.

249 Steve Lambakis, "Foreign Space Capabilities: Implications for U.S. National Security," 33.

250 *Worldwide Threat Assessment of the US Intelligence Community*, Daniel R. Coats, 2017, 7.

251 Micah Zenko, "Dangerous Space Incidents" (New York, NY: Council on Foreign Relations, 2014), 3, https://cfrd8-files.cfr.org/sites/default/

files/pdf/2014/04/CPA_ContingencyMemo_21.pdf.

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

253 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.

254 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.

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

256 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.

257 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/.

258 Michael Eisenstadt, "Iran's Lengthening Cyber Shadow," Research Notes 34 (Washington, DC: Washington Institute for Near East Policy, 2016), http://www.washingtoninstitute.org/uploads/Documents/pubs/ResearchNote34_Eisenstadt.pdf.

259 James A. Lewis, "Reconsidering Deterrence for Space and Cyberspace," in *Anti-Satellite Weapons, Deterrence and Sino-American Space Relations*, ed. Michael Krepon and Julia Thompson (Washington, DC: Stimson Center, 2013), 142, https://www.stimson.org/sites/default/files/file-attachments/Anti-satellite Weapons -The Stimson Center.pdf.

260 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.

NORTH KOREA

261 Roberts, *Spaceports of the World.*

262 Alex Lockie, "North Korea Looks to Be Preparing a Launch That Could Torpedo Talks and Bring a Full-on War with the US," Business Insider, April 3, 2018, https://www.businessinsider.com/north-korea-satellite-launch-could-torpedo-talks-bring-us-war-2018-4.

263 Missile Defense Project, "Taepodong-2 (Unha-3)," CSIS Missile Threat, June 15, 2018, https://missilethreat.csis.org/missile/taepodong-2/.

264 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/.

265 Gordon G. Chang, "Did North Korea Just Launch a Chinese Missile?," National Interest, February 15, 2017, http://nationalinterest.org/feature/did-north-korea-just-launch-chinese-missile-19459; Krishnadev Calamur, "How did North Korea's missile and nuclear tech get so good so fast?," *The Atlantic*, September 6, 2017, https://www.theatlantic.com/international/archive/2017/09/north-korea-tech/538959/.

266 Roberts, *Spaceports of the World*.

267 Donald J. Trump, "Press Conference by President Trump" (press conference, Capella Hotel, Singapore, June 12, 2018), https://www.whitehouse.gov/briefings-statements/press-conference-president-trump/.

268 Donald J. Trump and Kim Jong Un, "Joint Statement of President Donald J. Trump of the United States of America and Chairman Kim Jong Un of the Democratic People's Republic of Korea at the Singapore Summit," press release, June 12, 2018, The White House, https://www.whitehouse.gov/briefings-statements/joint-statement-president-donald-j-trump-united-states-america-chairman-kim-jong-un-democratic-peoples-republic-korea-singapore-summit/.

269 Joseph Bermudez and Victor Cha, "After Hanoi Summit: Rebuilding of Sohae Launch Facility," CSIS Beyond Parallel, March 5, 2019, https://beyondparallel.csis.org/hanoi-summit-rebuilding-sohae-launch-facility/.

270 Joseph Bermudez and Victor Cha, "North Korea Reportedly Renews Commitment to Dismantle the Sohae Launch Facility," CSIS Beyond Parallel, January 30, 2019, https://beyondparallel.csis.org/north-korea-reportedly-renews-commitment-dismantle-sohae-launch-facility/.

271 Bermudez and Cha, "After Hanoi Summit."

272 Roberts, *Spaceports of the World*.

273 Steven Lee Myers, "U.S. Calls North Korean Rocket a Failed Satellite," *New York Times*, September 15, 1998, https://www.nytimes.com/1998/09/15/world/us-calls-north-korean-rocket-a-failed-satellite.html.

274 Damian Grammaticas, "North Korea Rocket Launch Fails," BBC News, April 13, 2012, https://www.bbc.com/news/world-asia-17698438.

275 Missile Defense Project, "Taepodong-2 (Unha-3)."

276 "North Korea says it plans to launch many more satellites," *Taiwan News*, October 18, 2017, https://www.taiwannews.com.tw/en/news/3276934.

277 "Pyongyang Readies to Launch Satellite," *Korea JoongAng Daily*, December 27, 2017, http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=3042529&cloc=joongangdaily.

278 Missile Defense Project, "Taepodong-2 (Unha-3)."

279 Missile Defense Project, "North Korean Missile Launches & Nuclear Tests: 1984-Present," CSIS Missile Threat, November 29, 2017, https://missilethreat.csis.org/north-korea-missile-launches-1984-present/; Alexander Smith, "North Korea launched no missiles in 2018. But that isn't necessarily due to Trump," NBCNews.com, December 27, 2018, https://www.nbcnews.com/news/world/north-korea-launched-no-missiles-2018-isn-t-necessarily-due-n949971.

280 Missile Defense Project, "Hwasong-15 (KN-22)," CSIS Missile Threat, June 15, 2018, https://missilethreat.csis.org/missile/hwasong-15-kn-22/; Thomas G. Roberts, "Popular Orbits 101," CSIS Aerospace Security, November 30, 2017, https://aerospace.csis.org/aerospace101/popular-orbits-101/.

281 Weeden and Samson, eds., *Global Counterspace Capabilities*, 5–1.

282 "KCNA Report on DPRK's Accession to International Space Treaty and Convention," KCNA, March 12, 2009.

283 "Seventh Session of 12th SPA of DPRK Held," KCNA, April 1, 2013.

284 First Committee, "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.

285 Weeden and Samson, eds., *Global Counterspace Capabilities*, 5–1.

286 Joseph Bermudez, Victor Cha, and Lisa Collins, "Undeclared North Korea: Missile Operating Bases Revealed," CSIS Beyond Parallel, November 12, 2018, https://beyondparallel.csis.org/north-koreas-undeclared-missile-operating-bases/.

287 Joseph Bermudez, Victor Cha, and Lisa Collins, "Undeclared North Korea: The Sino-ri Missile Operating Base and Strategic Force Facilities," CSIS Beyond Parallel, January 21, 2019, https://beyondparallel.csis.org/undeclared-north-korea-the-sino-ri-missile-operating-base-and-strategic-force-facilities/.

288 Missile Defense Project, "No Dong 1," CSIS Missile Threat, June 15, 2018, https://missilethreat.csis.org/missile/no-dong/; David Wright, et al., *The Physics of Space Security*, 77.

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

290 Missile Defense Project,"Missiles of North Korea," CSIS Missile Threat, June 14, 2018, https://missilethreat.csis.org/country/dprk/.

291 David Wright et al., The Physics of Space Security, 125-130.

292 U.S. Congress, House, Committee on Homeland Security, Subcommittee on Oversight and Management Efficiency, Empty Threat or Serious Danger: Assessing North Korea's Risk to the Homeland, written statement of William R. Graham and Peter Vincent Pry, October 12, 2017, 1, http://docs.house.gov/meetings/HM/HM09/20171012/106467/HHRG-115-HM09-Wstate-PryP-20171012.pdf.

293 U.S. Congress, *Empty Threat or Serious Dange*r, 3.

294 Mun Dong Hui, "North Korean Propaganda Promotes EMP Attacks Using Nuclear Weapons," DailyNK, November 26, 2018, https://www.dailynk.com/english/north-korean-propaganda-promotes-emp-attacks-using-nuclear-weapons/.

295 Joby Warrick, Ellen Nakashima, and Anna Fifield, "North Korea Now Making Missile-ready Nuclear Weapons, U.S. Analysts Say," *Washington Post*, August 8, 2017, https://www.washingtonpost.com/world/national-security/north-korea-now-making-missile-ready-nuclear-weapons-us-analysts-say/2017/08/08/e14b882a-7b6b-11e7-9d08-b79f191668ed_story.html.

296 Lambakis, "Foreign Space Capabilities: Implications for U.S. National Security," 35.

297 U.S. Congress, *Empty Threat or Serious Danger*, 4.

298 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.

299 "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.

300 Ibid.

301 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.

302 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.

303 "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.

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

305 "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.

306 Lambakis, "Foreign Space Capabilities: Implications for U.S. National Security," 37.

307 Julian Ryall, "North Korea Doubles Its Cyber Warfare Team to 6,000 Troops," *Telegraph*, January 7, 2015, https://www.telegraph.co.uk/news/worldnews/asia/northkorea/11329480/North-Korea-doubles-its-cyber-warfare-team-to-6000-troops.html.

308 Michael S. Schmidt, Nicole Perlroth, and Matthew Goldstein, "F.B.I. says little doubt North Korea hit Sony," *New York Times*, January 7, 2015, https://www.nytimes.com/2015/01/08/business/chief-says-fbi-has-no-doubt-that-north-korea-attacked-sony.html.

309 Hyeong-wook Boo, "An Assessment of North Korean Cyber Threats" (presentation, 17th International Symposium on Security Affairs, Tokyo, Japan, July 25, 2016), 24, http://www.nids.mod.go.jp/english/event/symposium/pdf/2016/E-02.pdf.

310 Demetri Sevastopulo, "US Accuses North Korea over Global Cyber Crime Wave," *Financial Times*, September 6, 2018, https://www.ft.com/content/91453da8-b1de-11e8-99ca-68cf89602132.

OTHERS

311 Note: This figure corresponds to all space-faring nations other than the United States, China, Russia, Iran, and North Korea; Roberts, *Spaceports of the World*.

312 Statement for the Record: Worldwide Threat Assessment, 115th Cong. (March 6, 2018) (testimony of LTG Robert Ashley).

313 Note: Prior to 2018, Egyptian space activity had been lead by two state organizations: the National Authority for Remote Sensing and Space Science (NARSS) and the Academy of Scientific Research & Technology (ASRT). Both organizations were civil-focused; "Egypt," Space Gen-

eration Advisory Council, https://spacegeneration.org/regions/middle-east/egypt.

314 Al-Masry Al-Youm, "Sisi Passes Law Establishing Egyptian Space Agency," Egypt Independent, January 18, 2018, https://ww.egyptindependent.com/sisi-passes-law-establishing-egyptian-space-agency/.

315 Stephen Clark, "Egyptian observation satellite launched by Russian rocket," Spaceflight Now, February 21, 2019, https://spaceflightnow.com/2019/02/21/egyptian-observation-satellite-successfully-launched-by-russian-rocket/.

316 "EgyptSat-A," Gunter's Space Page, 2019, https://space.skyrocket.de/doc_sdat/egyptsat-a.htm.

317 Lisa O'Carroll, "Egypt accused of jamming al-Jazeera", *Guardian*, September 2, 2013, https://www.theguardian.com/media/2013/sep/02/egypt-accused-jamming-al-jazeera.

318 "Egypt jamming Al Jazeera's satellite signals," Al Jazeera, September 4, 2013, https://www.aljazeera.com/video/middleeast/2013/09/201393183256834226.html.

319 CSIS Aerospace Security, "Space Environment."

320 "Missions," Arianespace, accessed February 22, 2019, http://www.arianespace.com/missions/.

321 "France Joins 21st Century Space Race Fearing Future Conflict," Bloomberg, September 7, 2018, https://www.bloomberg.com/news/articles/2018-09-07/france-suspects-russian-space-attack-targeted-military-satellite.

322 Launchspace is a U.S.-based company and Astroscale is based in Japan. Jeff Foust, "Orbital debris removal company Astroscale raises $50 million," "Orbital Debris Solutions," Launchspace Technologies Corporation, http://launchspacetechnologies.com/orbital-debris-solutions/; Space News, October 31, 2018, https://spacenews.com/orbital-debris-removal-company-astroscale-raises-50-million/.

323 Note: Other partners include Airbus, Innovative Solutions in Space (ISIS), the Swiss Center for Electronics and Microtechnology (CSEM), National Institute for Research in Computer Science and Automation (INRIA), and Stellenbosch University; "RemoveDEBRIS," University of Surrey, https://www.surrey.ac.uk/surrey-space-centre/missions/removedebris; Jonathon Amos, "Space harpoon skewers 'orbital debris'," BBC, February 15, 2019, https://www.bbc.com/news/science-environment-47252304.

324 "Net successfully snares space debris," University of Surrey, September 19, 2018, https://www.surrey.ac.uk/news/net-successfully-snares-space-debris.

325 "RemoveDEBRIS," University of Surrey.

326 "Snap and Tsinghua," Surrey Space Centre, https://www.surrey.ac.uk/surrey-space-centre/missions/snap-and-tsinghua.

327 Dave Klingler, "Satellite-jamming becoming a big problem in the Middle East and North Africa," Ars Technica, March 28, 2012, https://arstechnica.com/science/2012/03/satellite-jamming-becoming-a-big-problem-in-the-middle-east/.

328 "Mango and Tango's Space Dance," Toulouse Cité de l'espace, September 15, 2010, http://en.cite-espace.com/space-news/mango-tango-s-space-dance/.

329 Joe McGauley, "NASA Is Going to Knock an Asteroid Out of Orbit in First-Ever Planetary Defense Test," Thrillist, February 5, 2019, https://www.thrillist.com/news/nation/nasa-attempt-to-knock-asteroid-out-of-orbit-2022; A. F. Cheng1 , A. S. Rivkin, and N. L. Chabot, "The Double Asteroid Redirection Test (Dart): New Developments," *50th Lunar and Planetary Science Conference 2019*, https://www.hou.usra.edu/meetings/lpsc2019/pdf/2424.pdf.

330 Hemant Singh, "Milestones in Indian Space Programmes," Jagranjosh.com, February 1, 2016, https://www.jagranjosh.com/general-knowledge/milestones-in-indian-space-programmes-1454322798-1.

331 "2015 Space Pioneer Award Was Presented to ISRO for Mars Orbiter Mission," ISRO, https://www.isro.gov.in/indias-space-policy-0.

332 Weeden and Samson, eds., Global Counterspace Capabilities, 6-4.

333 Note: Data limited to total launches from 1980 to 2018; Roberts, *Spaceports of the World*.

334 Doug Tsuruoka, "China Wants Missile Defenses To Stop India (And Kill Satellites)," *National Interest*, January 19, 2018, https://nationalinterest.org/blog/the-buzz/china-wants-missile-defenses-stop-india-kill-satellites-24132.

335 Franz-Stefan Gady, "India Test Fires Agni-V Nuclear-Capable ICBM," *Diplomat*, December 10, 2018, https://thediplomat.com/2018/12/india-test-fires-agni-v-nuclear-capable-icbm/.

336 Victoria Samson, "India's missile defense/anti-satellite nexus," The Space Review, May 10, 2010, http://www.thespacereview.com/article/1621/1.

337 Weeden and Samson, eds., *Global Counterspace Capabilities*, 5–1.

338 Missile Defense Project, "Missiles of India," CSIS Missile Threat, https://missilethreat.csis.org/country/india/.

339 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.

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

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

342 Ibid., 63.

343 Ibid., 64.

344 Israel Ministry of Science and Technology, "About the Israel Space Agency," Israel Space Agency, undated, accessed March 6, 2019, https://www.space.gov.il/en/About.

345 Isaac Ben-Israel and Zvi Kaplan, "New Frontiers," *From Modest Beginning to a Vibrant State*, Israel Ministry of Foreign Affairs, https://mfa.gov.il/MFA_Graphics/MFA%20Gallery/Israel60/ch7-6.pdf.

346 "Israel flying to moon for first lunar landing after SpaceX launch," NBC News, February 22, 2019, https://www.nbcnews.com/mach/science/israel-flying-moon-first-lunar-landing-after-spacex-launch-ncna974456.

347 As of March 9, 2019, Beresheet is estimated to land on the Moon on April 12, 2019.

348 John Horack, "First Private Lunar Spacecraft Shoots for the Moon," Space.com, February 2, 2019, https://www.space.com/43209-first-private-spacecraft-shoots-for-the-moon.html.

349 Barbara Opall-Rome, "US-Israel Arrow-3 Intercepts Target in Space," *Defense News*, December 10, 2015, https://www.defensenews.com/air/2015/12/10/us-israel-arrow-3-intercepts-target-in-space/.

350 Isaac Ben-Israel and Zvi Kaplan, "New Frontiers."

351 Japan, Basic Space Law (Law No.43 of 2008), Japan, May 28, 2008, http://stage.tksc.jaxa.jp/spacelaw/country/japan/27A-1.E.pdf.

352 Japan Ministry of Defense, *National Defense Program Guidelines for FY 2019 and beyond* (provisional translation), Japan Ministry of Defense, December 18, 2018, http://www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/20181218_e.pdf.

353 Toru Kasai, Mitsushuge Oda, and Takashi Suzuki, *Results of the ETS-7 Mission - Rendezvous Docking and Space Robotics Experiments* (Sengen, Tsukuba-shi, Ibaraki-ken, Japan: National Space Development Agency of Japan, 1999).

354 Charles Q. Choi, "Libya pinpointed as source of months-long satellite jamming in 2006," Space.com, April 9, 2007, https://www.space.com/3666-libya-pinpointed-source-months-long-satellite-jamming-2006.html.

355 "Thuraya Telecom Services affected by intentional jamming in Libya," Thuraya, February 25, 2011, http://www.thuraya.com/content/thuraya-telecom-services-affected-intentional-jamming-libya.

356 "Libya Source of Jamming of Lebanese News Channels: TRA," *Daily Star Newspaper*, February 23, 2011, http://www.dailystar.com.lb//News/Lebanon-News/2011/Feb-23/61826-libya-source-of-jamming-of-lebanese-news-channels-tra.ashx.

357 David Hencke and Owen Gibson, "Protest to Libya after Satellites Jammed," *Guardian*, December 3, 2005, https://www.theguardian.com/uk/2005/dec/03/politics.libya.

358 "Jazeera Tracks Jamming Signal to Libya Spy Building," Reuters, February 21, 2011, https://af.reuters.com/article/libyaNews/idAFLDE71K2CV20110221.

359 Kalbe Ali, "Rs4.7bn Allotted for Suparco Projects," *DAWN*, April 29, 2018, https://www.dawn.com/news/1404547.

360 "Space Race With India? Pakistan Plans Manned Mission With China's Help in 2022," News18, October 25, 2018, https://www.news18.com/news/world/pakistan-to-send-its-first-astronaut-into-space-in-2022-with-help-from-china-1920005.html.

361 Missile Defense Project, "Shaheen 3," CSIS Missile Threat, https://missilethreat.csis.org/missile/shaheen-3/.

362 Bill Gertz, "Moscow Accuses Ukraine of Electronic Attack on Satellite," Washington Free Beacon, March 17, 2014, https://freebeacon.com/national-security/moscow-accuses-ukraine-of-electronic-attack-on-satellite/.

363 Pavel Polityuk and Natalia Zinets, "Ukraine readies project to jam separatist broadcasting," Reuters, April 27, 2017, https://www.reuters.com/article/us-ukraine-crisis-propaganda/ukraine-readies-project-to-jam-separatist-broadcasting-idUSKBN17T1ST.

364 Tom Shales, "Cable's 'Captain Midnight' Apprehended," *Washington Post*, July 23, 1986, https://www.washingtonpost.com/archive/lifestyle/1986/07/23/cables-captain-midnight-apprehended/5d61712e-60c7-4351-8697-823761120593/.

365 Philip P. Pan, "Banned Falun Gong movement jammed Chinese satellite signal," *Washington Post*, July 9, 2002, https://www.washingtonpost.com/archive/politics/2002/07/09/banned-falun-gong-movement-jammed-chinese-satellite-signal/03fa9526-83a7-4ceb-9d5f-545fcd7e75a5/?utm_term=.d058f5edf7fc.

366 "Intelsat vows to stop piracy by Sri Lanka separatist group," Space News, April 18, 2007, http://spacenews.com/intelsat-vows-stop-piracy-sri-lanka-separatist-group/.

367 JJ McCoy, "Intelsat shuts down transponder hijacked by terrorists," Via Satellite, April 26, 2007, http://www.satellitetoday.com/uncategorized/2007/04/26/intelsat-shuts-down-transponder-hijacked-by-terrorists/.

368 Margaret Coker and Charles Levinson, "Rebels Hijack Gadhafi's Phone Network," *Wall Street Journal*, April 13, 2011, https://www.wsj.com/articles/SB10001424052748703841904576256512991215284.

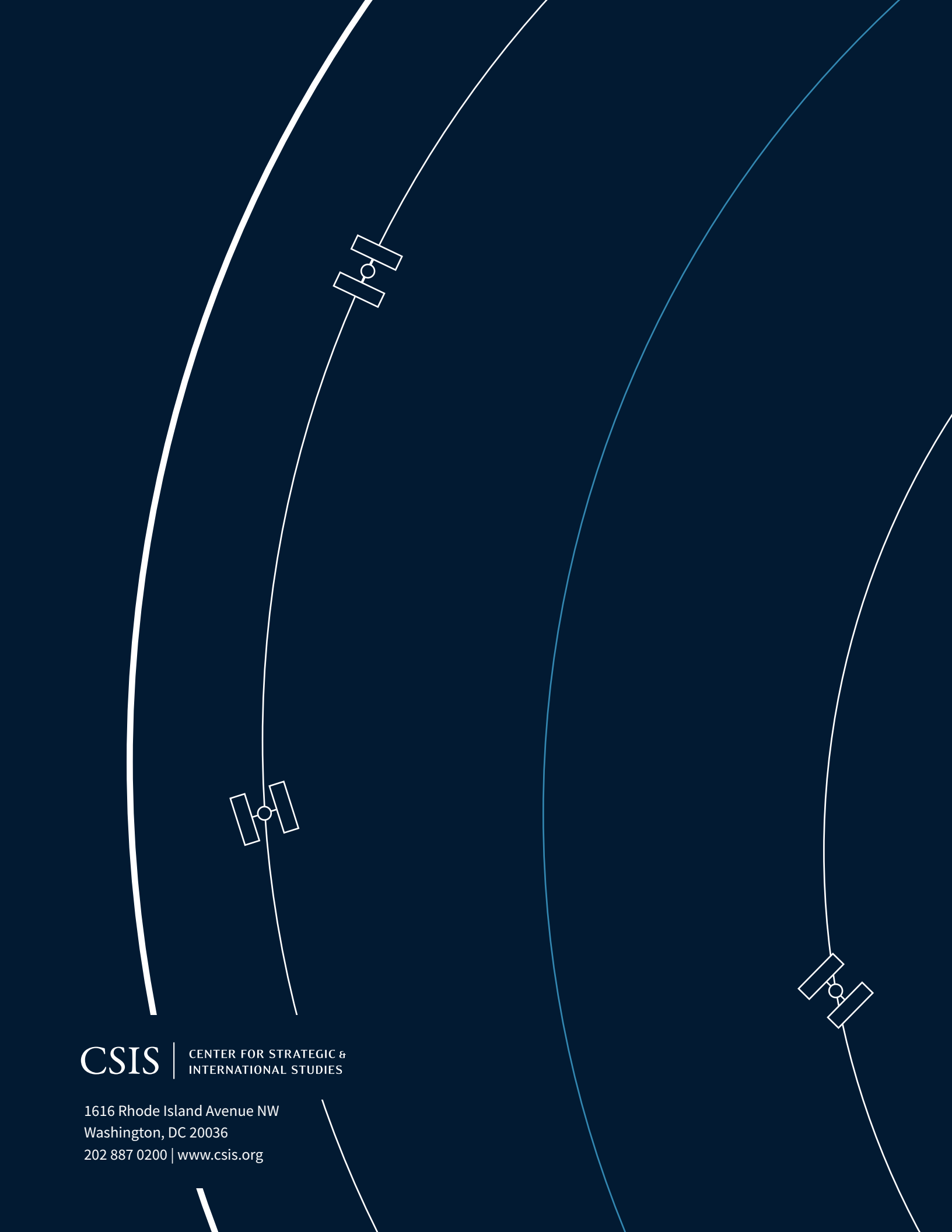
369 Hank Rausch, "Jamming Commercial Satellite Communications During Wartime: An Empirical Study," Proceedings of the Fourth IEEE International Workshop on Information Assurance, April 2006, http://ieeexplore.ieee.org/document/1610004/.

370 Craig Whitlock and Barton Gellman, "U.S. documents detail al-Qaeda's efforts to fight back against drones," *Washington Post*, September 3, 2013, https://www.washingtonpost.com/world/national-security/us-documents-detail-al-qaedas-efforts-to-fight-back-against-drones/2013/09/03/b83e7654-11c0-11e3-b630-36617ca6640f_story.html.

371 Ben Farmer, "British hacker admits stealing Pentagon satellite data," *Telegraph*, June 16, 2017, https://www.telegraph.co.uk/news/2017/06/16/british-hacker-admits-stealing-pentagon-satellite-data/.

372 J.M. Porup, "It's surprisingly simple to hack a satellite," Motherboard, August 21, 2015, https://motherboard.vice.com/en_us/article/bmjq5a/its-surprisingly-simple-to-hack-a-satellite.

373 "Mexican truckers fight highway robbery with armoured semis," *Malay Mail*, January 17, 2019, https://www.malaymail.com/news/life/2019/01/17/mexican-truckers-fight-highway-robbery-with-armored-semis/1713494.



CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

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