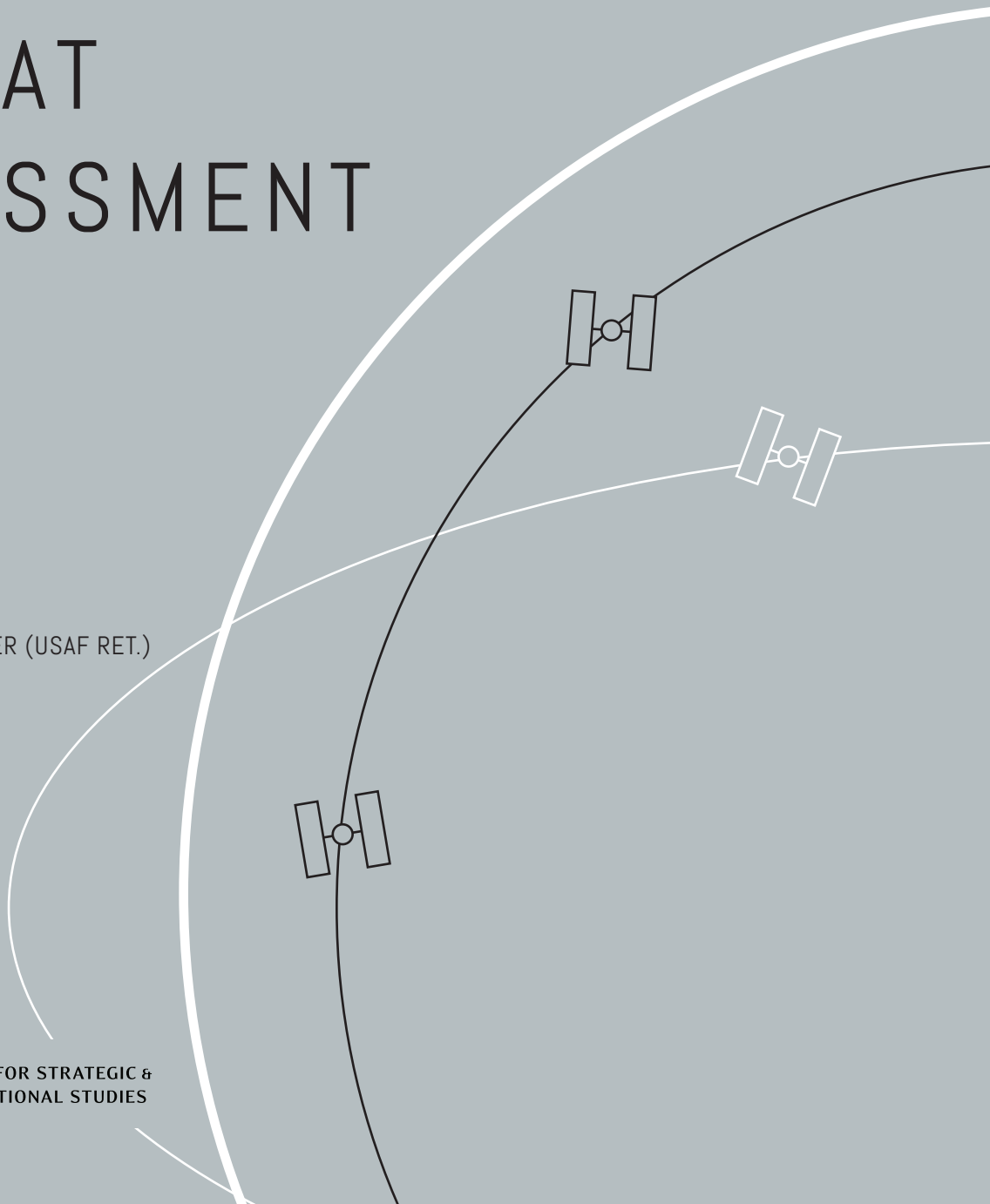
APRIL 2018

A REPORT OF
THE CSIS
AEROSPACE
SECURITY
PROJECT

SPACE THREAT ASSESSMENT 2018

Authors
TODD HARRISON
KAITLYN JOHNSON
THOMAS G. ROBERTS

Foreword
GEN. C. ROBERT KEHLER (USAF RET.)



CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

APRIL 2018

SPACE THREAT ASSESSMENT 2018

Authors
TODD HARRISON
KAITLYN JOHNSON
THOMAS G. ROBERTS

Foreword
GEN. C. ROBERT KEHLER (USAF RET.)

A REPORT OF THE
CSIS AEROSPACE SECURITY PROJECT

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

ABOUT CSIS

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

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

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

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

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

ABOUT ASP

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

ACKNOWLEDGMENTS

This assessment is made possible by the generous support of the Aerospace Industries Association. The authors would also like to thank Gen. C. Robert Kehler (USAF Ret.), Kyle Libby, Caroline Amenabar, Brian Weeden, Victoria Samson, and other experts from the Secure World Foundation.

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

CONTENTS

FOREWORD

AS THE WORLD'S LEADING SPACEFARING NATION, the United States has grown accustomed to relying on space capabilities as a cornerstone of our scientific endeavors, information age economy, and national security. Space is a key element of our national power and prestige, and decades of investment have yielded important warfighting and intelligence collection advantages for the United States and our allies and partners. Space capabilities make it possible for U.S. policymakers to know critical things about our world and adversaries that they would otherwise not know. Space capabilities enable the American way of warfare by making it possible for U.S. military commanders and forces to see the battlespace more clearly, communicate with certainty, navigate with accuracy, and strike with precision. Acknowledging this importance and consistent with prior administrations of both political parties, the current National Security Strategy recognizes that unimpeded access to and use of space is a vital national interest.

Our adversaries and potential adversaries have noted these significant advantages and have moved aggressively to field forces that can challenge our space capabilities from the ground, in space, and through cyberspace. From simple (and widely available and affordable) jammers to highly sophisticated antisatellite (ASAT) weapons, today the U.S. is facing serious threats in a domain that is increasingly an arena for conflict. Denying U.S. space capabilities is a central tenet of adversary strategies designed to diminish our prestige and raise the risks and costs of intervention in regional affairs.

This is not the first time the U.S. has had to consider challenges to our space capabilities. During the Cold War, we expected and planned for the Soviet Union to employ its significant capabilities to disrupt or destroy our space assets. However, today's problem is far more complex and potentially far greater in impact than the Cold War scenario. Given our dependence and that of our allies and partners on space, the loss of critical assets today could prove decisive to our ability to monitor critical events like missile launches or nuclear tests, or to successfully prosecute a military campaign.

Urgent action is needed. Countering this new reality requires a clear understanding of the threats and an approach highlighted by renewed national commitment and increased investment. On the pages that follow, you will find an excellent description of the threats. Compiled from open sources by CSIS, this paper provides a ready reference for all those desiring to know more about or charged with dealing with this significant national security problem. ○

GENERAL C. ROBERT KEHLER
United States Air Force (retired)

INTRODUCTION

THE UNITED STATES REMAINS A LEADER in the use of space for military purposes. From hunting down terrorists in remote parts of the world to securing a credible nuclear deterrent, the United States uses space systems across the full spectrum of military operations. Current 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, potential adversaries have taken notice. The U.S. military's dependence on space makes these systems a natural target for adversaries to exploit. Space is simultaneously a powerful enabler for the U.S. military and a critical vulnerability.

The [Defense] Department will prioritize investments in resilience, reconstitution, and operations to assure our space capabilities.

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

U.S. national security space systems are vulnerable to a wide array of threats, ranging from cyberattacks and jamming to direct-ascent anti-satellite (ASAT) missiles. While some U.S. space systems incorporate protections against certain types of attacks, all are vulnerable in certain ways. For example, the latest generation of protected satellite communications satellites, known as Advanced Extremely High Frequency (AEHF), incorporate a high degree of protection against jamming, spoofing, and other forms of electronic attack. But these satellites remain susceptible to kinetic attack, such as direct-ascent ASAT missiles or co-orbital weapons.

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 of others that can threaten U.S. space systems. The report focuses on four specific countries that pose the greatest risk for the United States: China, Russia, Iran, and North Korea. Following these case studies, 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, this report serves as an unclassified assessment that aggregates and highlights open-source information on counterspace capabilities for policymakers and the general public. ○

China and Russia challenge American power, influence, and interests, attempting to erode American security and prosperity… At the same time, the dictatorships of the Democratic People's Republic of Korea and the Islamic Republic of Iran are determined to destabilize regions, threaten Americans and our allies, and brutalize their own people.

NATIONAL SECURITY STRATEGY, THE WHITE HOUSE[2]

TYPES OF COUNTERSPACE WEAPONS

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[3]

COUNTERSPACE WEAPONS CAN VARY significantly in the types of effects they create, the level of technological sophistication required to conceive them, and the level of resources needed to develop and deploy 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

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 to do so, the satellite maneuvers to strike its target. Co-orbital ASATs can lie dormant in orbit for days or even years before being activated.[4] A key technology needed to make both direct-ascent and co-orbital ASAT weapons effective is the ability for the interceptor to sense and autonomously guide itself into a target satellite. This guidance technology requires a high level of technological sophistication and significant resources to test and deploy. Both are also enabled by associated targeting and command and control capabilities. An un-guided co-orbital ASAT, 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 on-board guidance and sophisticated targeting capabilities.

Ground stations can also be vulnerable to kinetic physical attacks by a variety of conventional military weapons, ranging from guided missiles and rockets at longer ranges to small arms fire at shorter ranges. Ground stations can be easier to attack in some respects because they are often highly visible, located in foreign countries, and are relatively soft targets. Ground stations can also be disrupted by attacking the electrical power grid, water supply, and the high-capacity communications lines that support them.

Kinetic physical attacks tend to have catastrophic and permanent effects on the satellites and ground stations they target. 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. Moreover, an attacker is likely to know if its attack is successful almost immediately because of effects that would be publicly visible, such as orbital debris.

NON-KINETIC PHYSICAL

NON-KINETIC COUNTERSPACE WEAPONS, such as lasers, high-powered microwaves, and electromagnetic pulse 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.[5] A laser is effective against a sensor on a satellite if it is within the field of view of that sensor, making it possible to attribute the attack to its approximate geographical origin. The attacker, however, will have limited ability to know if the attack was successful because it may not produce debris or other visible indicators.

THE USE OF A NUCLEAR WEAPON IN SPACE IS AN INDISCRIMINATE FORM OF NON-KINETIC PHYSICAL ATTACK.

A high-powered microwave (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" attack attempts to enter through small seams or gaps around electrical connections and shielding.[6] 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 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, the primary effect of a nuclear detonation in space is that it 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.[7]

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 satellite or receiver it is targeting. Jamming is usually completely reversible because once a jammer is turned off, communications can return to normal. Commercial and military satellites can be susceptible to both uplink and downlink jamming.[9] The uplink refers to the communications signal going up to the satellite, while the downlink is the signal that is sent from the satellite back to the ground.[10] An uplink jammer can interfere with the signal going up to a satellite, such as the command and control uplink, if it is within the field of view of the antenna on the satellite receiving the uplink.[11] Downlink jammers do not have to be as powerful as uplink jammers and target the users of a satellite by creating noise in the same frequency and at roughly the same power as the downlink signal from the satellite within the field of view of the receiving terminal's antenna.[12] Ground terminals with omnidirectional antennas, such as many Global Positioning System (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.

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 Space Command, noted that the U.S. military was jamming its own communications satellites an average of 23 times per month.[13]

Spoofing is a form of electronic attack where the attacker attempts to trick a receiver into believing a fake signal that the attacker's device produces is the real signal it is trying to receive. Spoofing the downlink from a satellite can be used to inject false or corrupted data into an adversary's communications systems. If an attacker successfully spoofs the command and control uplink signal to a satellite, it could take control of the satellite for nefarious purposes. Research has shown that even encrypted military GPS signals can be spoofed by a device that records the encrypted signal and rebroadcasts it with a slight delay. This specialized form of spoofing GPS signals, known as "meaconing,"[14] does not require cracking the GPS encryption because it merely rebroadcasts a time-delayed copy of the original signal. 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.

> Under severe stress situations, jamming can render all commercial [Satellite Communications, or SATCOM] and most defense SATCOM inoperable.
>
> DEFENSE SCIENCE BOARD TASK FORCE ON MILITARY SATELLITE COMMUNICATIONS AND TACTICAL NETWORKING[8]

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. While cyberattacks require a high degree of technological sophistica-

Example of a low-cost, commercially available GPS jammer

PHOTO FROM JAMMERSSL.COM

tion and 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 by contracting with groups of individuals that do have the necessary capabilities.

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, correspondingly, technological sophistication required. 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 the satellite's command and control system, the cyberattack 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.

THE TECHNOLOGY NEEDED TO JAM MANY TYPES OF SATELLITE SIGNALS IS COMMERCIALLY AVAILABLE AND RELATIVELY INEXPENSIVE.

NUMBER OF LAUNCHES IN 2017[16]

17

CHINA

OVERALL SPACE CAPABILITIES

...for countries that can never win a war with the United States by using the method of tanks and planes, attacking the U.S. space system may be an irresistible and most tempting choice.

WANG HUCHENG, CHINESE MILITARY ANALYST[15]

CHINA LAUNCHED ITS FIRST SATELLITE IN 1970. Only 33 years later it became the third nation to launch an astronaut.[17] Today, China is a major space power with a record of successful crewed space flights; two space stations, with plans for a third; lunar orbiters and a lunar rover; and a program to put Chinese taikonauts on the Moon.[18] To achieve these feats, China has an advanced family of rockets, the Long March series, that is used to launch satellites and the crewed Shenzhou spacecraft.

China has significant goals for its civil and military space systems. China's 2016 white paper on its space activities states that the country's vision is to "build China into a space power in all respects."[19] To accomplish this, China plans to "expedite the development of its space endeavors by continuing to enhance the basic capacities of its space industry."[20] As part of its mission to become a dominant actor in the domain, China has increased spending on space technologies and activities. In 2017, it was estimated that China spent almost $11 billion on space. This is the second most spending for any country on space activities; the United States spends the most at almost $48 billion.[21]

In addition to direct government investment in space, China has been attracting outside funding. In 2015, China and Russia partnered to launch a $200 million venture fund to incubate innovative technologies.[22] Private investors have also been actively supporting Chinese space start-ups, including a $182 million investment in a Chinese company called ExPace Technology, which to-date is "the largest investment in a non-U.S. space start-up."[23] One of the most active China-based investors, Tencent Holdings, has also invested in several U.S.-based space startups such as Moon Express, Planetary Resources, and World View Enterprises.[24]

To improve its space capabilities, China is focusing on many lines of effort, notably its rapid development and launch of both intelligence, surveillance, and reconnaissance (ISR) satellites and positioning, navigation, and timing (PNT) satellites. By 2020, China "plans to establish a global, 24-hour, all-weather earth remote sensing system and a global satellite navigation system."[25] With a PNT system of its own, China will rely less on the United States' GPS constellation for military and commercial applications. China is also experimenting with new capabilities in space, including such feats as launching the first ever quantum communications satellite in 2016.[26] China continues to increase its activity and experience in space, launching 31 payloads in 2017, second only to the United States in payloads launched that year.[27]

SPACE ORGANIZATION AND DOCTRINE

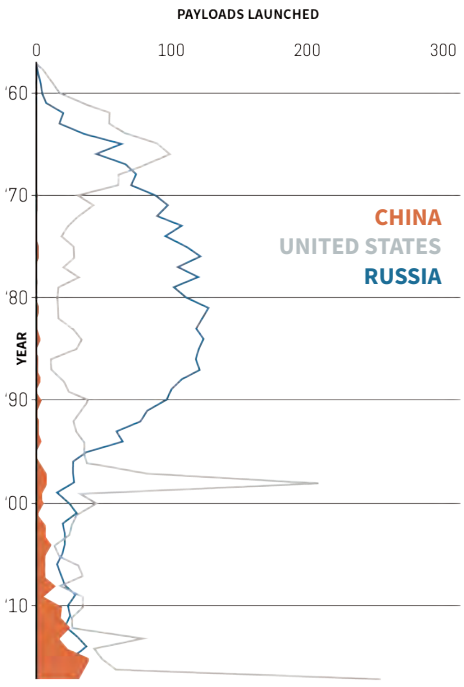
IN 2015, CHINA PUBLISHED a white paper on military strategy that states, "outer space and cyber space have become new commanding heights in strategic competition among all parties."[28] Many scholars believe that this statement represents China's formal designation of both space and cyberspace as new warfighting domains.[29] In recognition of the increasing importance of these two domains, China's military, the People's Liberation Army (PLA), created a new organization dedicated to both space and cyberspace in 2015. This new organization, called the Strategic Support Force (SSF), consolidates much of China's space and cyber capabilities into one central organization and bestows an elevated importance to space and cyberspace.[30] The mission of the SSF includes "coordinating and executing electronic warfare, space / counter-space and cyber warfare activities."[31] Although experts do not believe the SSF has full authority over the nation's arsenal of direct-ascent ASAT weapons, the SSF does appear to have control over other types of counterspace activities.[32]

China's Long March-2F rocket preparing for launch

FRED DUFOUR/AFP/GETTY IMAGES

PAYLOADS LAUNCHED PER YEAR

CHINA



SOURCE Space-Track.org[33]

In military writings, China sees both space and cyberspace as important elements of military power and views U.S. space and cyber assets as vulnerable.[34] Chinese military scholars write 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."[35] 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."[36] The PLA leadership is aware of China's growing reliance on space for its expanding military capabilities and reach. According to Chinese sources, achieving space superiority means China must en-

sure its ability to fully utilize its own space assets while simultaneously degrading, disrupting, or destroying its adversary's space capabilities.[37]

COUNTERSPACE WEAPONS

Kinetic Physical

China began testing its direct-ascent ASAT capabilities in the mid-2000s. The nation's first two tests of the SC-19 direct-ascent ASAT system occurred in 2005 and 2006 and were unsuccessful. In its third attempt in 2007, China destroyed one of its own satellites and produced a cloud of hazardous debris in low Earth orbit (LEO) that still threatens other satellites in that orbital regime today. Following the 2007 test, China conducted additional tests of the SC-19, although these were designed to not produce orbital debris.[38] In May 2013, China launched a new type of ASAT system, which Beijing claimed was intended to reach a height of 10,000 kilometers (km) to disperse a barium cloud for scientific research.[39] However, experts have suggested that this test was likely a high-altitude direct-ascent ASAT test that could reach satellites as high as geosynchronous orbit (GEO), which includes satellites used for missile warning, military communications, and ISR.[40] 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. China has also begun testing a new DN-3 ASAT missile capable of reaching higher orbits, with non-debris producing tests conducted in October 2015, December 2016, August 2017, and February 2018.[41] China may be developing three or more direct-ascent ASAT systems simultaneously, but it is not certain if each is intended to become operational or if some are intended to be missile interceptors.[42]

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.

China's 2007 ASAT Test

IN JANUARY 2007, China carried out a successful anti-satellite (ASAT) test, proving it could target and destroy space systems in low Earth orbit (LEO), such as imaging satellites. During this test, China successfully destroyed its own inactive meteorological satellite in polar orbit at an altitude of 865 km.[43]

Around 3,000 pieces of debris from this test that are large enough to track remain in space to this day. This debris threatens the safe operation of hundreds of other satellites in LEO, including the International Space Station.[44] To avoid collision, satellites must alter their trajectories, using up valuable fuel for unplanned maneuvers. This may lead to satellites running out of fuel sooner than anticipated and potentially having to end their missions early. Many other satellites in LEO, particularly cubesats and microsats, do not have maneuver capabilities and thus cannot avoid the debris.

China has also developed and launched several satellites for testing co-orbital capabilities. In 2008, a Chinese spacecraft deployed a miniature imaging satellite, the BX-1, that positioned itself in orbit around its mother spacecraft. After the successful deployment of the BX-1 and establishment of close orbit around the larger spacecraft, reports speculate that the BX-1 then maneuvered to intercept the International Space Station (ISS), passing within 45 km of the station without providing prior notification.[45] However, other accounts argue that the BX-1 was released by a spring-loaded device and was unable to be actively controlled until after it had passed the ISS.[46] While such technology may not be overtly counterspace, at a minimum it gives China the operational and technical expertise necessary to one day develop a co-orbital ASAT weapon.

In 2010, following the BX-1 test, China launched the SJ-12 satellite, which conducted a series of remote proximity maneuvers with an older Chinese satellite. Some have speculated that this mission was designed to test co-orbital jamming or other counterspace capabilities.[47] At one point, the SJ-12 satellite made contact with another satellite at low speed; however, this incident was "unlikely to have resulted in debris or

POSSIBLE NUCLEAR SITES IN CHINA

SOURCE Bulletin of the Atomic Scientists[51]

significant damage to either satellite."[48] 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.[49] In 2013, China reportedly tested its ability to use a robotic arm mounted on one satellite to seize another satellite,[50] although this has yet to be verified from publicly-available information.[52]

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,[53] the technology could potentially be further developed and used to damage or disable other satellites.[54] Similarly, China also deployed the Tianyuan-1 spacecraft in 2016, which according to Chinese press accounts, successfully tested the ability to refuel other satellites while in orbit.[55]

China has the largest standing army of any nation and over the past decade has significantly increased its military budget and modernized its conventional military forces.[56] In a conventional conflict, China could be capable of striking an adversary's satellite ground stations with ballistic missiles, cruise missiles, or long-range strike aircraft. And 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

China has made significant advances in non-kinetic forms of attack that can have physical effects on space systems from a distance. In a recent report, the U.S. Director of National Intelligence finds that China is making advances in directed energy technologies that can "blind or damage sensitive space-based optical sensors, such as those used for remote sensing or missile defense."[57] Chinese military and technical writings also reference directed energy as a key technology in successful counterspace

weapons.[58] For example, several Chinese scientists claimed to have successfully blinded a satellite in a 2005 test using a "50-100 [kilowatt] capacity mounted laser gun in Xinjiang province."[59] However, this claim cannot be confirmed through publicly-available information.

In 2006, reports surfaced that U.S. imagery satellites had been illuminated by lasers over Chinese territory.[60] Though much speculation surrounded these incidents, senior United States officials have stated that "China not only has the capability, but has exercised it."[61] Indeed, then-Director of the National Reconnaissance Office, Donald Kerr, acknowledged the incident over China, but stated that it did not "damage the U.S. satellite's ability to collect information."[62] 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.[63] As one China expert explained, "there are no serious fundamental barriers to China eventually obtaining an effective directed energy weapon system… the only fundamental barrier to learning these abstract elements and achieving a practical weapon capability is effort—time, will, and money."[64]

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."[65] However, adding a mobile HPM system to a satellite would require further reductions in size, weight, and power in addition to a number of other integration challenges unique to the space environment.

As a nuclear power with intercontinental ballistic missiles (ICBMs), China has the latent capability to launch a nuclear weapon into LEO. However, while China has the technology necessary to field a nuclear-armed ASAT weapon, it appears to be focusing its efforts in other areas.

CHINA HAS MADE THE DEVELOPMENT AND DEPLOYMENT OF SATELLITE JAMMING SYSTEMS A HIGH PRIORITY.

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.[66] 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.[67]

A paper from the China Electronic Technology Group Corporation proposes 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 identify U.S. satellites that would be particularly susceptible, such as "the AEHF (Advanced Extremely High Frequency), WGS (Wideband Global SATCOM), and GBS (Global Broadcast Service) satellite constellations."[68] Another Chinese technical paper provides 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.[69]

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.[70] 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.

Cyber

China has highly advanced cyber capabilities, many of which are run by the SSF in conjunction with their counterspace operations. Chinese hacks against secure

A building in Shanghai that allegedly housed a PLA hacking unit

PETER PARKS/AFP/GETTY IMAGES

2014 NOAA Satellite Hack

IN SEPTEMBER 2014, Chinese hackers attacked National Oceanographic and Atmospheric Administration's (NOAA) satellite information and weather systems. These critical systems are used by the U.S. military and other U.S. government agencies. 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.[76]

After the attack was made public, almost two months later, Rep. 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.[77]

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.[71] Chinese writings and research efforts indicate that in a conflict, it would attempt to conduct cyberattacks against U.S. satellites and ground stations.[72] As China expert David Chen has noted, "China's space system researchers already possess foundational knowledge that could be used for a cyber-electronic warfare counter-space R&D [Research and Development] program."[73]

China has already been implicated or suspected in several cyberattacks against U.S. satellites.[74] In October 2007 and again in July 2008, cyberattacks believed to originate in China targeted a remote sensing satellite operated by the U.S. Geological Survey called Landsat-7. Each attack caused 12 or more minutes of interference with ground station communications, but the attackers did not gain control over the satellite. In June and October of 2008, hackers also believed to be from China attacked NASA's Terra Earth observation satellite. In these attacks, the hackers "achieved all steps required to command the satellite but did not issue commands."[75]

CHINA HAS ALREADY BEEN IMPLICATED OR SUSPECTED IN SEVERAL CYBERATTACKS AGAINST U.S. SATELLITES.

NUMBER OF LAUNCHES IN 2017[79]

20

RUSSIA

OVERALL SPACE CAPABILITIES

We cannot just sit back and watch when others do it. I can only say that [ASAT research] is being conducted in Russia.

VLADIMIR POPOVKIN, DEPUTY DEFENSE MINSTER[78]

SINCE THE SUCCESSFUL LAUNCH OF SPUTNIK I ON OCTOBER 4, 1957, the Soviet Union, and subsequently the Russian Federation, has been one of the most dominant players in outer space. Russia remains a dominant actor in space today, particularly in space launch. Even the United States continues to use a Russian rocket engine, the RD-180, on one of its main space launch systems, the Atlas V.[80] However, the Russian space industrial base today pales in comparison to its Soviet predecessor, with a total space budget of only about $4 billion in 2016.[81] While a collection of design bureaus in the Soviet Union together constituted a majority of all global space launches in the first space age (1957 to 1991), Russia's modern International Launch Services (ILS)—an American-Russian commercial company known for its Angara and Proton rockets—now only makes up about 10% of the global market share.[82] In 2015, two separate organizations known as the Russian Federal Space Agency and United Rocket and Space Corporation, were consolidated into one megacorporation called Roscosmos.[83]

Although legacy Soviet space technology continues to provide an advantage for Russia today, the country has not continued to make advances in space at the same rate as it did during the Cold War. Many of Russia's satellite constellations deteriorated in the 1990s and 2000s due to a declining budget and crumbling economy; however, the country has maintained its global prominence in human spaceflight. 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 International Space Station (ISS).[84] 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 and the United States maintain a strong partnership in civil space; the two nations share training, communications, operations, and launch capabilities in support of the ISS.

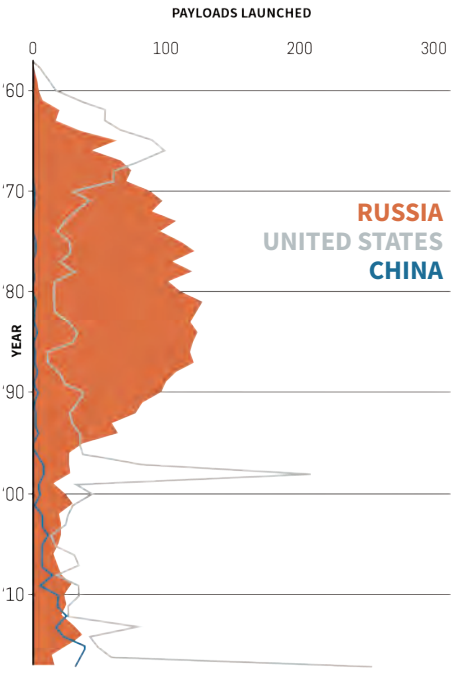
Russia is beginning to modernize many of its languishing space capabilities. The Global Navigation Satellite System (GLONASS) constellation of PNT satellites deteriorated through the 1990s, dropping to just 9 functional satellites out of the 24 that are necessary for global coverage. In 2011, Russia 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 network of satellites necessary for global coverage.[85] 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.[86, 87, 88]

SPACE ORGANIZATION AND DOCTRINE

DESPITE A DECLINE IN SOME AREAS after the fall of the Soviet Union, Russia remains a major player in military space and has extensive operational expertise from decades of space operations. Russia operates a comprehensive and well-organized space force, responsible for space object tracking and identification, space launch, and satellite operations.[89] Like China, Russia recently reorganized and consolidated its space forces. In 2011, it combined the air-defense and space forces into a new military branch known as the Aerospace Defense Forces (ADF). Then in 2015, it combined the Air Force and Aerospace Defense Forces into a new service—the Russian Aerospace Forces—with three sub-groups: the Air Force, Aerospace and Missile Defense Force, and Space Forces.[90] The mission of the Space Forces is to: monitor space objects, identify potential threats, prevent attacks from space, launch satellites, and control satellite operations (both military and civilian).[91]

RUSSIA HAS NOT CONTINUED TO MAKE ADVANCES IN SPACE AT THE SAME RATE AS IT DID DURING THE COLD WAR.

PAYLOADS LAUNCHED PER YEAR
RUSSIA



SOURCE Space-Track.org[92]

Russia believes that the militarization of outer space is a security threat and one of its "main external military danger[s]." The Russian military doctrine approved in 2010 states that "the securing of supremacy on land, at sea, and in the air and outer space will become decisive factors in achieving objectives."[93] According to the same document, one of the nation's "main tasks in deterring and preventing military conflicts" is to develop "an international treaty prohibiting the deployment of any types of weapons in outer space."[94] 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 UN Conference on Disarmament.[95] The United States dismissed the proposal as a "diplomatic ploy" and refused to sign on.[96] While Russia claims to view space as a peaceful domain and wants to prevent the development and use of weapons in space, its counterspace activities and weapons programs suggest otherwise.

COUNTERSPACE WEAPONS

Kinetic Physical

Russia continues to benefit from the Soviet Union's rich history of developing and operating anti-satellite weapons during the Cold War. With its first operational ASAT weapon program dating back to the early 1960s, the Soviet Union conducted extensive ASAT tests before its fall in December 1991. Soviet-era ASAT technologies give Russia a substantial advantage in the development of kinetic physical counterspace systems.

Two of the Soviet Union's verified ASAT weapon systems used co-orbital methods. The first program, Istrebitel Sputnikov (IS), meaning "satellite destroyer" in Russian, completed 20 tests from 1963 to 1982, and successfully destroyed several targeted satellites in orbit.[97] An announcement from April 1991 suggested a modified version of the IS system, named IS-MU, was also operational.[98] Like its predecessor, the IS-MU program was only de-

A Russian Krashukha-4 truck-mounted jamming system

VITALY V. KUZMIN

signed to take down satellites in LEO. Although the program officially ended in August 1993, its ground segment for identifying satellite targets on orbit continued to operate.[99]

In the early 1980s, the Soviet Union began developing its most powerful anti-satellite weapon yet, known as the Naryad. Also a co-orbital ASAT, the Naryad was designed to reach altitudes as high as 40,000 km, and could contain multiple individual warheads in a single launch, posing a threat to satellites in GEO.[100] The Naryad launch system—including the Rokot and Briz staging combination—is still used to launch satellites today.[101] The Naryad-era ground segment can track space objects in MEO and GEO and remains operational today; this tracking system is named Okno, which means "window" in Russian. Although Okno is in modern-day Tajikistan, control of the facility was transferred to Russia in the mid-2000s.[102] The system has undergone upgrades, and a 2016 report suggests that Okno can now detect objects as high as 50,000 km.[103] An Okno follow-on featuring more than ten new ground stations, called New Okno, is reportedly under construction within Russia's borders.[104]

At the center of co-orbital anti-satellite technologies is rendezvous and proximity operations (RPO). RPO involves moving a satellite close enough to a target to damage or destroy it. According to a 2018 Secure World Foundation report, Russia has engaged in a series of secretive RPO activities since 2013.[105] On several occasions the country has maneuvered space objects in LEO and GEO that were initially identified (incorrectly) as debris in the U.S. Space-Track catalog. These objects later appeared to maneuver and conduct proximity operations.[106] While modern-day Russian RPO activities are much different than the actual destruction of target satellites in the first IS program, Russia's current activities indicate that it is reviving its efforts in co-orbital counterspace technology development.

Russia's most recent kinetic ASAT tests have used direct-ascent technologies, representing a departure from the traditional co-orbital systems that dominated the Soviet approach. Intended for missile defense purposes, the PL-19 Nudol missile is capable of striking a satellite in LEO in much less time than a co-orbital ASAT. This system has been tested at least five times, but analysts disagree whether the launches should be considered ASAT tests, since the PL-19 Nudol missile system is also a missile interceptor.[107]

Other missiles in the Russian arsenal that are not specifically designed to strike satellites can also reach objects in space. The S-300 and S-400 missiles are surface-to-air missiles that are capable of "near space"[108] activity. In 2018, the Deputy Commander-in-Chief of the Russian Air Force said that the follow-on surface-to-air missile system, the S-500, would be available shortly.[109] The S-500 is expected to be capable of reaching altitudes of up to 600 km.[110] In 2013, the Russian government expressed interest in building an air-to-space system designed to "intercept absolutely everything that flies from space."[111] This view of a unified air, missile, and space defense is consistent with the organizational changes implemented by the Russian government in 2011 and 2015. In 2017, a Russian Aerospace Forces squadron commander confirmed that an ASAT missile had been designed for use with the MiG-31BM aircraft.[112] Some experts have interpreted the confirmation as a revival of the Soviet-era Kontakt program which was first tested in 1991.[113]

GPS Spoofing in the Black Sea

IN 2017, the U.S. Maritime Administration reported an apparent GPS spoofing attack in the Black Sea.[127] 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.[128]

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

Non-Kinetic Physical

Russia may have adapted Soviet-era non-kinetic systems for modern day use, just as it has adapted Soviet-era kinetic systems. The earliest anti-satellite research conducted by the Soviet Union prior to the original IS co-orbital ASAT program included several tests dedicated to understanding the destructive behavior of nuclear detonations at high altitudes. In October and November of 1962, Russia detonated three nuclear warheads approximately 400 km above the Earth's surface. These tests resulted in damage to other Soviet satellites, and the Soviets began working on a kill mechanism with more localized effects.[114] 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.[115]

In more recent years, Russia has actively developed and tested directed-energy counterspace weapons. In 2010, Russian reports announced the development of a laser ASAT weapon for use aboard a Beriev A-60 jet.[116] The system, now named Sokol Eshelon, meaning "Falcon Echelon," appears to be a revival of a Soviet system first developed in 1965.[117] Leaked photos from 2011 show the new A-60 system featuring a laser mounted on the top of the plane, suggesting that the laser fires upwards. An insignia on the side of the plane carries the name of the Soviet predecessor program and depicts a falcon with a laser beam striking a satellite that appears to be a space telescope. The laser was reportedly used in 2009 to illuminate a Japanese satellite at an altitude of 1,500 km.[118] 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.[119] A laser mounted on an A-60 aircraft could be capable of dazzling or blinding sensors on satellites; at sufficient power levels, the laser could also potentially damage other light- or heat-sensitive physical components on a satellite, such as solar arrays. An airborne laser platform is also more challenging for an adversary to locate and avoid because it is inherently mobile.

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).[120] Laser ranging involves sending short laser pulses to a satellite in order to observe the pulses' reflection and determine the distance between it and the observation site.[121] Although there is no evidence showing that Russia's ILRS lasers have been used to dazzle satellites, some of the same technologies used for laser ranging could be adapted for a counterspace system.[122]

Electronic

Recent conflicts in Ukraine and Syria demonstrate that Russia retains advanced electronic attack capabilities, despite some analysts' claims that Russia's ability to jam and spoof satellites has declined since 1991.[123] 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,

Beriev A-60

Insignia on a laser-equipped Beriev A-60 featuring a laser striking a satellite and the words "Sokol Eschelon"

IVAN SAVITSKY/ROVSPOTTERS, RUSSIANPLANES.NET

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.[124] A video leaked in 2015 confirms 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.[125] In 2016, the Russian military began installing a GPS jamming 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.[126]

Cyber

Russia's cyber capabilities are among the most advanced in the world, and it uses these capabilities on a regular basis in all domains. Since 2007, a Russian-speaking group of hackers, likely linked to the Russian government, has stolen satellite data used by government groups, militaries, and embassies around the world.[129] This group, known for using malware called Turla, attacks older communications satellites that still use unencrypted data links.[130]

Outside of the space domain, Russia is regularly accused of engaging in extreme cyberwarfare. In 2007, Russia was blamed for cyberattacks against Estonia which paralyzed online banking services, government communications, and Estonian media outlets.[131] Similarly, Ukraine has sustained thousands of Russian cyberattacks throughout the Crimean conflict over the past few years.[132] 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.[133] The governments of the United Kingdom, France, Germany, Kyrgyzstan, and Georgia have each accused Russia of similar cyberattacks.[134] Given Russia's prolific use of cyberattacks in other domains, Russia's cyber capabilities likely pose a significant threat to space systems as well.

NUMBER OF LAUNCHES IN 2017[136]

0

IRAN

OVERALL SPACE CAPABILITIES

Tehran views its space program as critical to its national pride and the fight against its external enemies.

STEVE LAMBAKIS[135]

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.[137] Iran still has a relatively weak space industrial base, especially given evidence suggesting that a portion of Iran's space technologies were adapted from Russian and North Korean counterparts.[138] 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,[139] and the Safir-2, which has been used as a space launch vehicle.[140] Iran maintains two domestic space launch facilities in the northeastern Semnan Province. Iran has also secured an agreement to use the Baikonur Cosmodrome in Kazakhstan for space launch.[141]

Iran successfully launched its first domestically-manufactured satellite on a Safir-2 rocket in 2009, and has vowed to put a human in space by 2025.[142] 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 mouse, turtle, and worms. In 2013, Iran stated that it had sent a monkey into space.[143] 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, "the base is aimed at securing the country's space facilities and monitoring space objects, especially satellites that pass overhead."[144] The defense minister also revealed that Iran is using satellites to control unmanned aerial vehicles (UAVs) so that it can operate over longer distances and is not limited by line-of-sight radio links.[145]

Iranian Safir rocket

VAHIDREZA ALAI/AFP/GETTY IMAGES

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.[146] The agency is under the oversight of the Ministry of Information and Communication 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.[147] The head of the Iranian Space Agency serves as the secretary of the Supreme Space Council.[148]

Little is publicly known about Iran's doctrine for space and counterspace operations, but evidence suggests that Iran believes its ability "to deny the United States the ability to use space in a regional conflict" is critical to its security.[149] 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. A Council on Foreign Relations report from 2014 assesses that, "Iran undertakes more purposeful interference with U.S. military and commercial space systems using lasers and jammers than any other country."[150]

IRAN'S EFFORTS IN SPACE ARE OFTEN VIEWED AS A THINLY-VEILED COVER FOR ITS DEVELOPING BALLISTIC MISSILE PROGRAM.

COUNTER-SPACE 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 kinetic ASAT capability. 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 kinetic ASAT weapon, such as onboard sensors that could steer 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.

Non-Kinetic Physical

Iran may have acquired and used a laser dazzling or

blinding counterspace system 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."[151] 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, and Iran's capabilities in this area remain highly uncertain based on publicly available information.

The 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."[152] 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.[153] However, 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 ASAT weapon.

Electronic

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 an 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.[154]

In another incident in 2010, Iran jammed British Broadcasting Corporation (BBC) and VOA satellite 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.[155]

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."[156] Attackers can interfere with satellite signals through a process called "meaconing" in which a legitimate GPS signal is spoofed and rebroadcast at a higher power level. This method of attack does not require cracking the encryption used in the military GPS signal because the data in the signal is not modified but rather is simply rebroadcasted with a slight time delay.[157] The U.S. government did not verify Iran's claims, but if true, they represent a significant counterspace capability that could be used to thwart U.S. precision-guided weapons in the future.

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.[158] 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.[159] Iran's sophisticated cyber capabilities suggest that it could employ cyberattacks on space systems as well.

NUMBER OF LAUNCHES IN 2017[161]

0

NORTH KOREA

OVERALL SPACE CAPABILITIES

NORTH KOREA HAS AN ACTIVE SPACE PROGRAM that is closely related to its missile program, which has made significant progress in recent years. Still, many experts doubt that the few satellites launched by North Korea perform all of the functions that the North Korean government claims.[162] 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/or Pakistan.[163]

North Korea successfully orbited its first satellite in December 2012 after three failed attempts in July 2006, April 2009, and April 2012. The successful launch used the Unha-3, a launch vehicle believed to be a variant of the Taepodong-2 ICBM. In its fifth test in February 2016, it successfully placed a second satellite in orbit.[164] 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. Moreover, North Korea has publicly stated its intent to continue launching remote sensing satellites and to send an unmanned mission to the moon within a decade.[165]

In parallel with its space program, North Korea has also made significant progress in developing and testing ballistic missiles. Under the Kim Jong-Un regime, it has ramped up its missile test program from 6 ballistic missile launches in 2012 to 25 launches in 2017.[166] Its November 2017 test of the Hwasong-15 ICBM followed a lofted trajectory to reach an apogee of 4,475 km and a range of 950 km. If the same vehicle with the same payload were launched on a range-maximizing trajectory, it could reach virtually any location in the United States.[167] Based on publicly available information, however, it is not clear whether North Korea has developed the re-entry

> North Korea is a critical threat to the United States and our allies in Northeast Asia and is our hardest intelligence collection target.
>
> LTG ROBERT ASHLEY, DIRECTOR, DEFENSE INTELLIGENCE AGENCY[160]

North Korea launches multiple ballistic missiles on March 6, 2017
STR/AFP/GETTY IMAGES

vehicle technology that would be necessary to deploy a conventional or nuclear warhead on its long-range missiles.

SPACE ORGANIZATION AND DOCTRINE

LITTLE IS KNOWN ABOUT NORTH KOREA'S DOCTRINE or operational concepts for the use of space and counterspace capabilities. Most of the country's military capabilities appear to be focused on ensuring the survival of the regime and deterring foreign aggression, and it maintains "a stridently confrontational posture against the United States."[168] When the regime speaks publicly about space, it is usually in the context of peaceful programs and its right to be a space power. 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.[169]

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 various 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.[170] Like Iran, 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 could create a debris field that complicates future operations for the target satellite and any other satellites in a similar orbit.

Non-Kinetic Physical

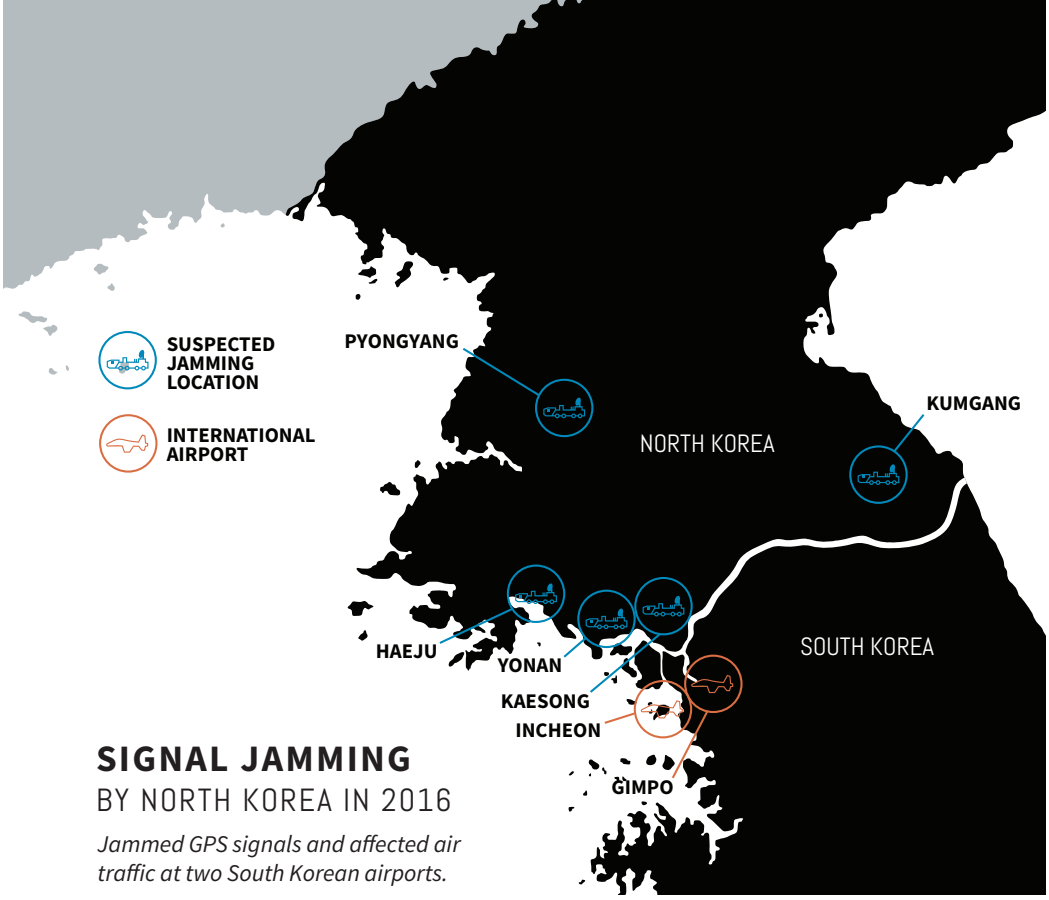
There is some evidence that North Korea may be developing or has already acquired non-kinetic physical counterspace weapons such as a nuclear EMP device.[171] However, the technology necessary for more sophisticated directed-energy weapons, such as lasers that can dazzle or blind the sensors on satellites, requires a level of technology that North Korea is unlikely to possess anytime soon.[172] Another country, particularly China or Russia, could provide such capabilities to North Korea, but there is no publicly available evidence to suggest this has occurred.

Given its existing ballistic missile and nuclear capabilities, North Korea could theoretically launch a nuclear weapon into space and detonate it.[173] Using a nuclear weapon in this manner does not require re-entry vehicle technology like a nuclear-armed ICBM would. Tests of nuclear weapons in space were banned by the 1963 Partial Test Ban Treaty, but North Korea is not a signatory to this treaty.[174]

In a written statement to Congress in 2017, the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack (the EMP Commission) offered evidence that North Korea may be developing an EMP weapon. 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."[175]

Electronic

North Korea has acquired and is actively using electronic forms of attack against U.S. 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."[176] These downlink



SIGNAL JAMMING
BY NORTH KOREA IN 2016

Jammed GPS signals and affected air traffic at two South Korean airports.

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.[177]

In the years since, North Korea has repeatedly used its GPS jamming capabilities against South Korea. More GPS jamming occurred in December 2010 and again in March 2011. The 2011 incident lasted 10 days and coincided with an annual U.S.-Korean military exercise.[178] Jamming occurred again in April 2012, disrupting air traffic at Incheon and Gimpo International Airports, and forcing flights to use alternative navigation systems.[179] In 2016, South Korea complained to the United Nations Security Council that the North was again jamming GPS signals across the border, with the jamming coming from five areas in North Korea: Pyongyang, Kaesong, Haeju, Yonan county, and Mount Kumgang.[180]

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."[181] The jammers are mounted on mobile platforms and are operated intermittently, and 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 the North's GPS jamming is a violation of the 1953 armistice agreement,[182] no effective measures have been undertaken to date to curb this activity.

NORTH KOREA HAS ACQUIRED AND IS ACTIVELY USING ELECTRONIC FORMS OF ATTACK AGAINST U.S. SPACE SYSTEMS.

Cyber

General Vincent Brooks, 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.[183] Under the Kim Jong-Un regime, North Korea has exercised these 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.[184] 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.[185] 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.

OTHERS

MANY OTHER COUNTRIES AND NON-STATE ACTORS have developed technologies that are dual-use in nature or are directly intended as counterspace weapons. This section explores the counterspace capabilities beyond those available to China, Russia, Iran, and North Korea. It highlights how some of these counterspace weapons have been employed so far and the challenges they create.

KINETIC PHYSICAL

Israel

Israel's Arrow missile defense system could in theory be used as an ASAT capability. 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.[186] Though not a true ASAT test, like those conducted by China in 2007, the test proved that Israel could have a latent ASAT capability.

India

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. In 2010, the then-head of India's Defense Research and Development Organization, Director General V.K. Saraswat also stated that India would "validate the anti-satellite capability on the ground through simulation," rather than active tests.[187] While they have reiterated that they possess ASAT capabilities, Indian officials do not want to weaponize space or create harmful debris in orbit from a test.[188]

Indian Angi-V ballistic missile system
RAVEENDRAN/AFP/GETTY IMAGES

Japan

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.[189] 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.

Europe

Several European countries have developed space capabilities that can also be used for co-orbital ASAT weapon. In 2000, a British satellite was launched in the same faring as a much larger Chinese satellite. Despite some technical difficulties, the British spacecraft successfully maneuvered within 2km of the Chinese satellite.[190] In 2010, two Swedish satellites, dubbed Mango and Tango, performed a series of rendezvous maneuvers and formation flying.[191]

DUE TO THE DUAL-USE NATURE OF MANY SPACE TECHNOLOGIES, EVEN BENIGN SPACE CAPABILITIES CAN BE VIEWED BY OTHERS AS COUNTERSPACE WEAPONS.

NON-KINETIC PHYSICAL

India and Pakistan

Both India and Pakistan have nuclear weapons and ballistic missiles that can reach orbital altitudes. India has several medium-range and intercontinental ballistic missiles that could be used to deliver a nuclear weapon into orbit.[192] Similarly, 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.[193] However, neither country has indicated that it plans to test or field such a system.

ELECTRONIC

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."[194] Five years later, in 2011, Thuraya's satellite communications were once again jammed over Libya.[195] This time, Thuraya claimed the attack was intended "as a revolt continued against Libyan leader Muammar Gaddafi."[196]

Egypt

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 company was forced to change frequencies several times to avoid the jamming. According to Al Jazeera, it traced the jammers back to at least four Egyptian military installations near Cairo.[197]

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."[198] Similarly, a Chinese spiritual organization, Falun Gong, spoofed Chinese satellite television broadcasts in 2002, replacing the footage with its own video.[199]

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.[200] The Washington Post, in 2013, reported on concerns within the Defense Intelligence Agency (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.[201]

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. Indeed, 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."[202]

CYBER

Non-State Actors

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.[203] The attack caused Intelsat to shut down the satellite transponder after more than a year of unauthorized use.[204] 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.[205] 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.[206]

CONCLUSION

ON OCTOBER 13, 1959, just two years after the launch of Sputnik 1, the United States conducted the first test of an ASAT system, launching a Bold Orion missile from a B-47 bomber at one of its own satellites.[208] In the years that followed this initial counterspace experiment, both the United States and the Soviet Union tested a variety of ASAT systems that could hold each other's space assets at risk. These kinetic capabilities were never used in anger because each side recognized the destabilizing effects an attack in space would have on the balance of power on Earth. Today, the U.S. military is reliant on space across the full spectrum of conflict, from counter-terrorism operations to high-end combat against a near-peer adversary. The threats to space systems have also metastasized, with a variety of counterspace systems proliferating to more nations and even non-state actors.

> I believe that any domain that humans move into will be subject to conflict... conflict will move into space.
>
> GEN. JOHN HYTEN[207]

As this report has discussed, other nations are making significant advances in counterspace capabilities. China is a rising space power that is progressing steadily in the development and testing of direct-ascent and co-orbital kinetic ASAT systems. China already appears to possess advanced jamming, spoofing, directed-energy, and cyberattack capabilities that can threaten a variety of U.S. space systems. Russia continues to benefit from legacy Soviet-era capabilities, but its space systems deteriorated significantly in the 1990s and 2000s. However, Russia is now modernizing its space capabilities, and has revived or developed new counterspace weapons of nearly all types, including direct-ascent and co-orbital kinetic ASAT systems, an airborne lasing platform, advanced jamming and spoofing capabilities, and formidable cyberattack capabilities. While North Korea and Iran still lag far behind Russia and China in their space and counterspace capabilities, each is making quick progress thanks to technology transfers from other countries and their own ballistic missile programs. For now, the main threats from both North Korea and Iran in space appear to be non-kinetic forms of attack, such as jamming, spoofing, and cyberattacks. These types of counterspace weapons tend to be cheaper, require less technological sophistication, and are already within the reach of some non-space actors as well.

Deterrence can be particularly challenging for non-kinetic, electronic, and cyber methods of attack because these can be more difficult to detect and attribute and can have reversible effects. As this report has shown, some of these counterspace weapons are already being used against the United States and its allies and partners on a regular basis. While it is difficult to imagine a world without the advantages space provides to the military and daily life, it is far too easy to take these capabilities for granted. The growing threats against U.S. space systems and the ground stations that support them require immediate attention and action from policymakers.

APPENDIX I

LIST OF ACRONYMS USED

ADF	Russian Aerospace Defense Forces
AEHF	Advanced Extremely High Frequency
ASAT	Anti-Satellite
BBC	British Broadcasting Corporation
DIA	Defense Intelligence Agency
EMP	Electromagnetic Pulse
GEO	Geosynchronous Orbit
GBS	Global Broadcast Service
GLONASS	Global Navigation Satellite System (Russia)
GPS	Global Positioning System
HPM	High Powered Microwave
ICBM	Intercontinental Ballistic Missile
ILRS	International Laser Ranging Service
ILS	International Launch Services
IS	Istrebitel Sputnikov (Russia)
ISR	Intelligence, Surveillance, and Reconnaissance
ISS	International Space Station
JCPOA	Joint Comprehensive Plan of Action
km	Kilometers
LEO	Low Earth Orbit
MEO	Medium Earth Orbit
MMW	Millimeter Wave
NASA	National Aeronautics and Space Administration
NOAA	National Oceanographic and Atmospheric Administration
PLA	People's Liberation Army (China)
PNT	Positioning, Navigation, and Timing
R&D	Research & Development
RF	Radio Frequency
RPO	Rendezvous and Proximity Operations
SATCOM	Satellite Communications
SSF	Strategic Support Force (China)
UAV	Unmanned Aerial Vehicle
UHF	Ultra High Frequency
USSTRATCOM	United States Strategic Command
VOA	Voice of America
WGS	Widespread Global SATCOM (Satellite Communications)

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 B.S. and an M.S. in aeronautics and astronautics.

KAITLYN JOHNSON is a research associate for the Aerospace Security Project at CSIS. Her work focuses on supporting ASP's space security and air dominance and long-range strike research portfolios. Previously, she has written on the U.S. Air Force budget, escalation and deterrence dynamics in the second space age, ultra-low-cost access to space, and defense acquisition trends. Ms. Johnson was formerly a program manager and research associate for the Defense-Industrial Initiatives Group (DIIG) at CSIS. She holds an M.A. from American University in U.S. foreign policy and national security studies with a concentration in defense and space security, and a B.S. from the Georgia Institute of Technology.

THOMAS G. ROBERTS is a program coordinator and research assistant for the Aerospace Security Project at CSIS. His research interests include international collaboration in space, satellite system architecture analysis, and space policy in the United States Congress. Mr. Roberts is the host and executive producer of *Moonstruck*, a podcast about the history of human spaceflight. He holds a B.A. in astrophysical sciences with honors and an undergraduate certificate in Russian studies from Princeton University. In 2015, Mr. Roberts was named a Harry S. Truman Scholar.

ENDNOTES

INTRODUCTION

1 U.S. Department of Defense, "Summary of the 2018 National Defense Strategy," 6, https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

2 The White House, "National Security Strategy of the United States of America," December 2017, 2, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

TYPES OF COUNTERSPACE WEAPONS

3 U.S. Department of Defense, "Summary of the 2018 National Defense Strategy," 3.

4 U.S. Congress, Office of Technology Assessment, *Anti-Satellite Weapons, Countermeasures, and Arms Control* (Washington,, DC: Government Printing Office, September 1985), 7.

5 Brian Garino and Jane Gibson, "Space System Threats," in *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.

6 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/publications/Physics_of_space_security.pdf.

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

8 Defense Science Board, United States Department of Defense, *Task Force on Military Satellite Communication and Tactical Networking: Executive Summary* (Washington, DC: Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, March 2017), 2, https://www.acq.osd.mil/dsb/reports/2010s/DSB-MilSatCom-FINALExecutiveSummary_UNCLASSIFIED.pdf.

9 Brian Garino and Jane 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 Brian Garino and Jane Gibson, "Space System Threats,"274-275.

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, "Innovation: GNSS Spoofing Detection," GPS World, June 1, 2013, http://gpsworld.com/innovation-gnss-spoofing-detection-correlating-carrier-phase-with-rapid-antenna-motion/.

CHINA

15 Wang Hucheng, "The U.S. Military's 'Soft Ribs' and Strategic Weaknesses," Beijing Xinhua Honk Kong Service, July 5, 2005, quoted in Ashley J. Tellis, "China's Military Space Strategy," Survival 49, no. 3 (July 31, 2007), 49.

16 This figure does not include a failed launch attempt that was included in the original source. "Orbital Launches of 2017," Gunter's Space Page, accessed April 5, 2018, http://space.skyrocket.de/doc_chr/lau2017.htm.

17 "A brief history of China in space," *The Telegraph*, August 24, 2011, http://www.telegraph.co.uk/news/science/space/8719848/A-brief-history-of-China-in-space.html.

18 Andrew Jones, "Launch of first Chinese space station module delayed to 2020," GBTIMES, March 5, 2018, https://gbtimes.com/launch-of-first-chinese-space-station-module-delayed-to-2020?cat=chinas-space-program.

19 The State Council Information Office, "China's Space Activities in 2016," Xinhua, The State Council Information Office, December 27, 2016, http://www.xinhuanet.com/english/china/2016-12/27/c_135935416.htm.

20 Ibid.

21 "Global Space Industry Dynamics" (Alexandria, VA: Bryce Space and Technology, 2017), 3, https://brycetech.com/downloads/Global_Space_Industry_Dynamics_2017.pdf.

22 Jonathan Vanian, "Russia and China partner on $200 million venture fund, incubator for Russian tech companies," Fortune, April 21, 2015, http://fortune.com/2015/04/21/russia-china-venture-incubator/.

23 "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.

24 Ibid., 11.

25 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.

26 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.

27 Space-Track.org, accessed February 22, 2018, https://space-track.org/.

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

29 Kevin Pollpeter, et al., "The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations," 3-4.

30 Bill Gertz, “Chinese Military Revamps Cyber Warfare, Intelligence Forces,” The Washington Free Beacon, January 27, 2016, http://freebeacon.com/national-security/chinese-military-revamps-cyber-warfare-intelligence-forces/.

31 Tate Nurkin, “Implications of China’s Military Modernization,” *Hearing before the U.S. China Economic and Security Review Commission*, February 15, 2018, 8, https://www.uscc.gov/sites/default/files/Nurkin_Written Testimony.pdf.

32 Kevin Pollpeter, et al., “The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations,” 29.

33 Space-Track.org.

34 Bruce W. MacDonald, Dennis Blair, Dean Cheng, Karl Mueller, and Victoria Samson, “Crisis Stability in Space: China and Other Challenges,” (Washington, DC: The Foreign Policy Institute, 2016), 16, http://media.wix.com/ugd/b976eb_360f1f449cdd41799e49a35c231472fa.pdf.

35 “China Military Encyclopedia, Second Edition,” People’s Liberation Army National Defense University (Beijing, PRC: Encyclopedia of China Publishing House, 2007), 211; quoted in Bruce W. MacDonald, et al., “Crisis Stability in Space: China and Other Challenges,” 29.

36 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.

37 Kevin Pollpeter, et al., “The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations,” 7.

38 U.S.-China Economic and Security Review Commission, “2015 Report to Congress of the U.S.-China Economic and Security Review Commission,” 294.

39 “中国再次高空科学探测试验：高度更高数据更多”, 中国新闻网, May 14, 2013, http://www.chinanews.com/gn/2013/05-14/4817925.shtml.

40 U.S.-China Economic and Security Review Commission, “2015 Report to Congress of the U.S.-China Economic and Security Review Commission,” 293.

41 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/.

42 Brian Weeden and Victoria Samson, eds., *Global Counterspace Capabilities: An Open Source Assessment*, 1-11, https://swfound.org/counterspace/.

43 T.S. Kelso, “Analysis of the 2007 Chinese ASAT Test and the Impact of its Debris on the Space Environment,” Center for Space Standards & Innovation, http://celestrak.com/publications/AMOS/2007/AMOS-2007.pdf.

44 Brian Weeden, “2007 Chinese Anti-Satellite Test Fact Sheet,” Secure World Foundation, November 23, 2010, https://swfound.org/media/9550/chinese_asat_fact_sheet_updated_2012.pdf.

45 U.S.-China Economic and Security Review Commission, “2015 Report to Congress of the U.S.-China Economic and Security Review Commission,” 295.

46 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.

47 U.S.-China Economic and Security Review Commission, “2015 Report to Congress of the U.S.-China Economic and Security Review Commission,” 295.

48 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.

49 Kevin Pollpeter, et al., “The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations,” 10.

50 U.S.-China Economic and Security Review Commission, “2015 Report to Congress of the U.S.-China Economic and Security Review Commission,” 295.

51 Hans M. Kristensen and Robert S. Norris, “Worldwide Deployments of Nuclear Weapons, 2017,” *Bulletin of the Atomic Scientists*, 73, no. 5, (August 31, 2017), 290.

52 Brian Weeden and Victoria Samson, eds., “Global Counterspace Capabilities,” 1-2.

53 Ibid.

54 “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/.

55 “China announces success in technology to refuel satellites in orbit,” Xinhua, June 30, 2016, http://www.xinhuanet.com/english/2016-06/30/c_135479061.htm.

56 “Chapter Two: Comparative defence statistics,” in *The Military Balance 2017*, International Institute for Strategic Studies, (London: Routledge, 2017), 19 - 26.

57 U.S. Congress, Senate, Select Committee on Intelligence, *Worldwide Threat Assessment of the US Intelligence Community*, written statement of Daniel R. Coats, February 13, 2018, 13, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

58 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.

59 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.

60 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/.

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

62 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.

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

64 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.

65 Richard D. Fisher Jr., "China's Progress with Directed Energy Weapons," 9.

66 "Annual Report to Congress: Military Power of the People's Republic of China 2007," Office of the Secretary of Defense, 2007, 21, https://fas.org/nuke/guide/china/dod-2007.pdf.

67 U.S.-China Economic and Security Review Commission, "2015 Report to Congress of the U.S.-China Economic and Security Review Commission," 297-298.

68 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.

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

70 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.

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

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

73 David D. Chen, "Opening Statement of Mr. David Chen," 75.

74 Ibid.

75 Ibid.

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

77 Mary Pat Flaherty, Jason Samenow and Lisa Rein, "Chinese hack U.S. weather systems, satellite network," *The 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.

RUSSIA

78 "Russia Developing Its Own Antisatellite Systems - Deputy Minister," *Interfax AVN*, March 5, 2009; quoted in Jana Honkova, *The Russian Federation's Approach to Military Space and Its Military Space Capabilities* (Washington, DC: George C. Marshall Institute, 2013).

79 This figure does not include a failed launch attempt that was included in the original source. "Orbital Launches of 2017," Gunter's Space Page, accessed April 5, 2018, http://space.skyrocket.de/doc_chr/lau2017.htm.

80 Todd Harrison, Andrew Hunter, Kaitlyn Johnson, Thomas G. Roberts and Evan Linck, "Beyond the RD-180" (Washington, DC: Center for Strategic and International Studies, 2017), https://aerospace.csis.org/beyond-rd-180/.

81 "Global Space Industry Dynamics," 3.

82 Ibid., 9.

83 Elizabeth Howell, "Roscosmos: Russia's Space Agency," Space.com, January 29, 2018, https://www.space.com/22724-roscosmos.html.

84 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.

85 Yuri Urlichich, Valery Subbotin, Grigory Stupak, Vyacheslav Dvorkin, Alexander Povalyaev, Sergey Karutin, and Rudolf Bakitko, "GLONASS Modernization," GPS World, November 1, 2011, http://gpsworld.com/glonass-modernization-12232/.

86 "На противника посмотрят с двухметровой объективностью," Газета Коммерсанть, July 28, 2018, https://www.kommersant.ru/doc/3049019.

87 "The ExoMars Programme 2016-2020," European Space Agency, http://exploration.esa.int/mars/46048-programme-overview/.

88 Asif Siddiqi, "Russia's Space Program Is Struggling Mightily," Slate Magazine, March 21, 2017, http://www.slate.com/articles/technology/future_tense/2017/03/russia_s_space_program_is_in_trouble.html.

89 "Aerospace Defence Forces," Ministry of Defence of the Russian Federation, http://eng.mil.ru/en/structure/forces/cosmic.htm.

90 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/.

91 "Aerospace Defence Forces."

92 Space-Track.org, accessed February 22, 2018, https://space-track.org/.

93 President of the Russian Federation, "2010 Military Doctrine of the Russian Federation," February 5, 2010, http://carnegieendowment.org/files/2010russia_military_doctrine.pdf.

94 Ibid.

95 "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/.

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

97 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.

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

99 Ibid.

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

101 Gunter Dirk Krebs, "Briz," Gunter's Space Page, October 27, 2017, http://space.skyrocket.de/doc_stage/briz.htm.

102 "Okno ELINT complex in Tajikistan is becoming Russian," Ferghana News, April 17, 2006, 2018, http://enews.fergananews.com/article.php?id=1390.

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

104 "Russia to Deploy New Systems to Detect Space Objects," The Times of India, November 18, 2014, https://fas.org/spp/military/program/track/okno.pdf#page=5.

105 Brian Weeden and Victoria Samson, eds., "Global Counterspace Capabilities," 2-2.

106 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/2839/1.

107 Bill Gertz, "Russia Flight Tests Anti-Satellite Missile," The Washington Free Beacon, December 2, 2015, http://freebeacon.com/national-security/russia-conducts-successful-flight-test-of-anti-satellite-missile/; Bill Gertz, "Russia Flight Tests Anti-Satellite Missile," The Washington Free Beacon, May 28, 2016, http://freebeacon.com/national-security/russia-flight-tests-anti-satellite-missile/.

108 "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/.

109 John Pike, "S-500 Samoderzhets," Global Security, https://www.globalsecurity.org/military/world/russia/s-500.htm.

110 Steve Lambakis, "Foreign Space Capabilities: Implications for U.S. National Security," National Institute for Public Policy (Fairfax, VA: National Institute Press, 2017), 28, http://www.nipp.org/wp-content/uploads/2017/09/Foreign-Space-Capabilities-pub-2017.pdf.

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

112 Alexander Zudin, "Russia to deploy anti-satellite weapon on MiG-31BM," IHS Jane's Missiles & Rockets, February 22, 2017, http://www.janes.com/article/68102/russia-to-deploy-anti-satellite-weapon-on-mig-31bm.

113 Jana Honkova, The Russian Federation's Approach to Military Space and Its Military Space Capabilities (Arlington, VA: George C. Marshall Institute, 2013).

114 Asif A. Siddiqi, "The Soviet Co-Orbital Anti-Satellite System," 230.

115 U.S. Library of Congress, Congressional Research Service, *High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments*, by Clay Wilson, RL32544 (2008); 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.

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

117 Ibid.

118 David Cenciotti, "Russia has completed ground tests of its high-energy Airborne combat Laser System," The Aviationist, October 5, 2016, https://theaviationist.com/2016/10/05/russia-has-completed-ground-tests-of-its-high-energy-airborne-combat-laser-system/.

119 Alexei Mikhailov, "Пиу-пиу," Lenta.ru, May 22, 2013, https://lenta.ru/articles/2012/11/13/russianlaser/.; "Beams away: Russia boosts airborne combat laser program," Russia Today, November 19, 2012, https://www.rt.com/op-ed/soviet-airborne-laser-restarted-600/.

120 "International Laser Ranging Service (ILRS)," November 14, 2017, https://ilrs.cddis.eosdis.nasa.gov/network/stations/index.html.

121 "Satellite Laser Ranging (SLR)," International Earth Rotation and Reference Systems Service, https://www.iers.org/IERS/EN/Science/Techniques/slr.html.

122 Brian Weeden and Victoria Samson, eds., "Global Counterspace Capabilities," 2-27.

123 "Modern Russian Electronic Warfare," Leonardo DRS, Spring 2016, http://www.leonardodrs.com/sitrep/q1-2016-the-invisible-fight/modern-russian-electronic-warfare/.

124 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," InformNapalm.org (English), 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," InformNapalm.org (English), November 16, 2017, https://informnapalm.org/en/russian-r-330zh-jammer-detected-7-km-from-the-contact-line-in-donbas/.

125 Elias Groll, "Spy Planes, Signal Jammers, and Putin's High-Tech War in Syria," *Foreign Policy*, October 06, 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," The Conversation, October 8, 2015, https://theconversation.com/how-syria-is-becoming-a-test-bed-for-high-tech-weapons-of-electronic-warfare-48779.

126 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.; "Silent Protector: Russia Develops Hi-Tech Jammer to Block Enemy Electronics," Sputnik International, August 25, 2016, https://sputniknews.com/russia/201608251044633778-russia-jammer-electronics/.

127 "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/.

128 Dana Goward, "Mass GPS Spoofing Attack in Black Sea?" The Maritime Executive, July 11, 2017, https://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea#gs.QGC4kZ8.

129 Ellen Nakashima, "Russian hacker group exploits satellites to steal data, hide tracks," *The 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.

130 "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.

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

132 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.

133 David E. Sanger, "Putin Ordered 'Influence Campaign' Aimed at U.S. Election, Report Says," *The New York Times*, January 06, 2017, https://www.nytimes.com/2017/01/06/us/politics/russia-hack-report.html.

134 UK Blames Russia for Cyberattack, Says Won't Tolerate Disruption," CNBC, February 15, 2018, https://www.cnbc.com/2018/02/15/uk-blames-russia-for-cyberattack-says-wont-tolerate-disruption.html; Gordon Corera, "How France's TV5 Was Almost Destroyed by 'Russian Hackers'," BBC News, October 10, 2016, http://www.bbc.com/news/technology-37590375; Justin Huggler, "Russia Cyber Attack on Germany a 'form of Warfare'," The Telegraph, March 1, 2018, https://www.telegraph.co.uk/news/2018/03/01/russia-cyber-attack-germany-form-warfare/; Robert Mackey, "Are 'Cyber-Militias' Attacking Kyrgyzstan?" The New York Times, February 5, 2009, https://thelede.blogs.nytimes.com/2009/02/05/are-cyber-militias-attacking-kyrgyzstan/; Tom Espiner, "Georgia Accuses Russia of Coordinated Cyberattack," CNET, August 11, 2008, https://www.cnet.com/news/georgia-accuses-russia-of-coordinated-cyberattack/.

IRAN

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

136 This figure does not include a failed launch attempt that was included in the original source. "Orbital Launches of 2017," Gunter's Space Page, accessed April 5, 2018, http://space.skyrocket.de/doc_chr/lau2017.htm.

137 Aria Bendix, "Iran Claims It Launched a Satellite-Carrying Rocket Into Space," The Atlantic, July 27, 2017, https://www.theatlantic.com/news/archive/2017/07/iran-claims-it-launched-a-satellite-carrying-rocket-into-space/535161/.

138 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.

139 "Shahab-3," MissileThreat: CSIS Missile Defense Project, Center for Strategic and International Studies, August 9, 2016, https://missilethreat.csis.org/missile/shahab-3/.

140 "Safir," MissileThreat: CSIS Missile Defense Project, Center for Strategic and International Studies, October 16, 2017, https://missilethreat.csis.org/missile/safir/.

141 "Iran signs space launch agreement with Kazakhstan," Spacewatch Middle East, April 2016, https://spacewatchme.com/2016/04/iran-signs-space-launch-agreement-kazakhstan/.

142 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), 146-147, https://www.rand.org/pubs/monographs/MG1103.html.

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

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

145 Adam Kredo, "Iran satellite launch prompts fear of long range ballistic missile attack," The Washington Free Beacon, August 31, 2016, http://freebeacon.com/national-security/iran-satellite-launch-prompts-fear-long-range-ballistic-missile-attack/.

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

147 "Iranian Space Agency," Iran Watch: Tracking Iran's Unconventional Weapon Capabilities, Wisconsin Project on Nuclear Arms Control, August 31, 2009, https://www.iranwatch.org/iranian-entities/iranian-space-agency.

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

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

150 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.

151 Scott Peterson and Payam Faramarzi, "Exclusive: Iran hijacked U.S. drone, says Iranian engineer," The Christian Science Monitor, December

15, 2011, https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer.

152 U.S. Congress, Senate, Select Committee on Intelligence, *Worldwide Threat Assessment of the US Intelligence Community*, written statement of Daniel R. Coats, May 11, 2017, 7, https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf.

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

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

155 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.

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

157 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/.

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

159 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.

NORTH KOREA

160 LTG Robert Ashley, "Worldwide Threat Assessment of the US Intelligence Community," *Testimony before the Armed Services Committee*, March 6, 2018, 3, https://www.armed-services.senate.gov/imo/media/doc/Ashley_03-06-18.pdf.

161 "Orbital Launches of 2017," Gunter's Space Page, accessed April 5, 2018, http://space.skyrocket.de/doc_chr/lau2017.htm.

162 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/.

163 Gordon G. Chang, "Did North Korea Just Launch a Chinese Missile?," The 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/.

164 "Taepodong-2 (Unha-3)," MissileThreat: CSIS Missile Defense Project, Center for Strategic and International Studies, August 8, 2016, https://missilethreat.csis.org/missile/taepodong-2/.

165 "North Korea plans moon landing," News.com.au, August 5, 2016, http://www.news.com.au/technology/science/space/north-korea-plans-moon-landing/news-story/23d8ea776a6b7d7add19bdabf9f3e957.

166 "North Korean Missile Launches & Nuclear Tests: 1984-Present," MissileThreat: CSIS Missile Defense Project, Center for Strategic and International Studies, November 29, 2017, https://missilethreat.csis.org/north-korea-missile-launches-1984-present/.

167 "Hwasong-15 (KN-22)", MissileThreat: CSIS Missile Defense Project, Center for Strategic and International Studies, December 7, 2017, https://missilethreat.csis.org/missile/hwasong-15-kn-22/.

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

169 Brian Weeden and Victoria Samson, eds., "Global Counterspace Capabilities," 5-1.

170 Ibid.

171 William R. Graham, "North Korean Nuclear EMP Attack: An Existential Threat," 38 North, June 2, 2017, https://www.38north.org/2017/06/wgraham060217/?utm_source=38+North+Bulletin+060217&utm_campaign=38+North&utm_medium=email#_ftnref2.

172 David Wright, Laura Grego, and Lisbeth Gronlund, *The Physics of Space Security: A Reference Manual*, 125-130.

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

174 "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.

175 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, 3, http://docs.house.gov/meetings/HM/HM09/20171012/106467/HHRG-115-HM09-Wstate-PryP-20171012.pdf.

176 "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.

177 Ibid.

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

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

180 "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.

181 "Massive GPS jamming attack by North Korea."

182 "South Korea tells U.N. that North Korea GPS jamming threatens boats, planes."

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

184 Michael S. Schmidt, Nicole Perlroth, and Matthew Goldstein, "F.B.I. says little doubt North Korea hit Sony," *The 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.

185 Hyeong-wook Boo, "An Assessment of North Korean Cyber Threats" (paper presented at the *17th International Symposium on Security Affairs: The Kim Jong Un Regime and the Future Security Environment Surrounding the Korean Peninsula*, Tokyo, Japan, July 25, 2016), 24, http://www.nids.mod.go.jp/english/event/symposium/pdf/2016/E-02.pdf

OTHERS

186 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/.

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

188 Brian Weeden and Victoria Samson, eds., "Global Counterspace Capabilities," 6-1.

189 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).

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

191 "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/.

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

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

194 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.

195 "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.

196 "Thuraya satellite telecom says jammed by Libya," Reuters, February 24, 2011, https://www.reuters.com/article/libya-satphone-thuraya/thuraya-satellite-telecom-says-jammed-by-libya-idUSLDE71N2CU20110224.

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

198 Tom Shales, "Cable's 'Captain Midnight' Apprehended," The Washington Post, July 23, 1986, https://www.washingtonpost.com/archive/lifestyle/1986/07/23/cables-captain-midnight-apprehended/5d61712e-60c7-4351-8697-823761120593/?utm_term=.827023c6b5e3.

199 Philip P. Pan, "Banned Falun Gong movement jammed Chinese satellite signal," The 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.

200 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/?reload=true.

201 Craig Whitlock and Barton Gellman, "U.S. documents detail al-Qaeda's efforts to fight back against drones," The 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?utm_term=.c15349e5bf7b.

202 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.

203 "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/.

204 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/.

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

206 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

CONCLUSION

207 John Hyten, "Space Wars: Are We Prepared for The Next Domain of Warfare?" (panel discussion, Ronald Reagan Presidential Library, Simi Valley, December 1, 2017).

208 John Pike, "Bold Orion Weapons System 199 (WS-199B)," Global Security, https://www.globalsecurity.org/space/systems/bold-orion.htm.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

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