Promoting Cooperative Solutions for Space Sustainability

Global Counterspace Capabilities: An Open Source Assessment

April 2018

Editors

Brian Weeden
Director of Program Planning
Secure World Foundation

Victoria Samson
Washington Office Director
Secure World Foundation

ABOUT SECURE WORLD FOUNDATION

Secure World Foundation (SWF) is a private operating foundation dedicated to the secure and sustainable use of space for the benefit of Earth and all its peoples. SWF engages with academics, policy makers, scientists, and advocates in the space and international affairs communities to support steps that strengthen global space sustainability. It promotes the development of cooperative and effective use of space for the protection of Earth's environment and human security.

ABOUT THE EDITORS

Dr. Brian Weeden is the Director of Program Planning for Secure World Foundation and has nearly two decades of professional experience in space operations and policy.

Dr. Weeden directs strategic planning for future-year projects to meet the Foundation's goals and objectives, and conducts research on space debris, global space situational awareness, space traffic management, protection of space assets, and space governance. Dr. Weeden also organizes national and international workshops to increase awareness of and facilitate dialogue on space security, stability, and sustainability topics. He is a member and former Chair of the World Economic Forum's Global Future Council on Space Technologies and is also a member of the Advisory Committee on Commercial Remote Sensing (ACCRES) to the National Oceanic and Atmospheric Administration (NOAA).

Prior to joining SWF, Dr. Weeden served nine years on active duty as an officer in the United States Air Force working in space and intercontinental ballistic missile (ICBM) operations. As part of U.S. Strategic Command's Joint Space Operations Center (JSpOC), Dr. Weeden directed the orbital analyst training program and developed tactics, techniques and procedures for improving space situational awareness.

Respected and recognized as an international expert, Dr. Weeden's research and analysis have been featured in The New York Times, The Washington Post, National Public Radio, USA Today, The BBC, Fox News, China Radio International, The Economist, The World Economic Forum's Annual Meeting in Davos, academic journals, presentations to the United Nations, and testimony before the U.S. Congress.

Ms. Victoria Samson is the Washington Office Director for Secure World Foundation and has twenty years of experience in military space and security issues.

Before joining SWF, Ms. Samson served as a Senior Analyst for the Center for Defense Information (CDI), where she leveraged her expertise in missile defense, nuclear reductions, and space security issues to conduct in-depth analysis and media commentary. Prior to her time at CDI, Ms. Samson was the Senior Policy Associate at the Coalition to Reduce Nuclear Dangers, a consortium of arms control groups in the Washington, D.C. area, where she worked with Congressional staffers, members of the media, embassy officials, citizens, and think-tanks on issues surrounding dealing with national missile defense and nuclear weapons reductions. Before that, she was a researcher at Riverside Research Institute, where she worked on war-gaming scenarios for the Missile Defense Agency's Directorate of Intelligence.

Known throughout the space and security arena as a thought leader on policy and budgetary issues, Ms. Samson is often interviewed by multinational media outlets, including the New York Times, Space News, and NPR. She is also a prolific author of numerous op-eds, analytical pieces, journal articles, and updates on missile defense and space security matters.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

Acronym	Long Form
AAD	Advanced Area Defense
ABL	Airborne Laser
ABM	Anti-Ballistic Missile
ACCRES	Advisory Committee on Commercial Remote Sensing
ADRV	Advanced Debris Removal Vehicle
AIS	Automated Identification System
AMS	Academy of Military Sciences
ANGELS	Automated Navigation and Guidance Experiment for Local Space
APT	Advanced Persistent Threat
ASAT	Antisatellite
ATBM	Anti-Tactical Ballistic Missile
AWACS	Airborne Early Warning and Control Systems
BMD	Ballistic Missile Defense
C2	Command-and-Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CASC	China Aerospace Science and Technology Corporation
CASIC	China Aerospace Industrial Corporation
CCAFS	Cape Canaveral Air Force Station
CCD	Charge-coupled Device
CCS	Counter Communications System
CDI	Center for Defense Information
CMOS	Complementary Metal-oxide Semiconductor
CNE	Computer Network Exploitation
COMSAT	Communications Satellite
DA-ASAT	Direct-Ascent ASAT
DARPA	Defense Advanced Research Project Agency
DART	Demonstration for Autonomous Rendezvous Technology
DDOS	Distributed Denial of Service
DEW	Directed Energy Weapons
DHS	Department of Homeland Security
DNS	Domain Name System

DRDO	Defence Research and Development Organisation
DSC	Defensive Space Control
ECS	Environmental Control Systems
EKV	Exoatmospheric Kill Vehicle
ELINT	Electronic Intelligence
EMP	Electromagnetic Pulse
EW	Electronic Warfare
FBI	Federal Bureau of Investigation
FSB	Federal Security Service
FY	Fiscal Year
GBI	Ground-based Interceptor
GEO	Geostationary Earth Orbit
GLONASS	Global Navigation Satellite Systems
GMD	Ground-based Missile Defense
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
GSO	Geosynchronous Orbit
GSSAP	Geostationary Space Situational Awareness Program
HTK	Hit-to-kill
ICBM	Intercontinental ballistic missile
ICS	Industrial Control Systems
IRBM	Intermediate Range Ballistic Missile
IRGC	Islamic Revolutionary Guard Corps
ISR	Intelligence, Surveillance, and Reconnaissance
ISRO	Indian Space Research Organisation
ITU	International Telecommunication Union
JICSpOC	Joint Interagency Combined Space Operations Center
JNWC	Joint Navigation Warfare Center
JSpOC	Joint Space Operations Center
KCNA	Korean Central News Agency
KKV	Kinetic Kill Vehicle
KW	Kilowatt
LEO	Low-Earth Orbit
LPAR	Large Phased-Array Radar

MEO	Medium Earth Orbit
Mi-TEx	Micro-satellite Technology Experiment
MITM	Man-in-the-middle
MUBLCOM	Multiple Path Beyond Line of Site Communication
NASA	National Aeronautics and Space Administration
NAVIC	Navigation with Indian Constellation
NAVWAR	Navigation Warfare
NOAA	National Oceanic and Atmospheric Administration
NOTAM	Notice to Airmen
NPT	Nuclear Non-Proliferation Treaty
NSA	National Security Agency
NSDC	National Space Defense Center
OCS	Offensive Counterspace
OSC	Offensive Space Control
PAD	Prithvi Air Defence
PDV	Prithvi Defence Vehicle
PGM	Precision-Guided Munitions
PNT	Positioning, Navigation, and Timing
RAT	Remote Access Tool
RDT&E	Research, Development, Testing, and Evaluation
RF	Radiofrequency
RPO	Rendezvous and Proximity Operations
SAM	Surface-to-air Missile
SAR	Synthetic Aperture Radar
SAST	Shanghai Academy of Spaceflight Technology
SATCOM	Satellite Communications
SBSS	Space-Based Surveillance System
SCADA	Supervisory Control and Data Acquisition
SDI	Strategic Defense Initiative
SIGINT	Signals Intelligence
SLBM	Submarine-launched Ballistic Missile
SLR	Satellite Laser Ranging
SLV	Space Launch Vehicle
SPR	Space Strategic Portfolio Review

SSA	Space Situational Awareness
SWF	Secure World Foundation
TEL	Transporter-erector-launcher
THAAD	Terminal High Altitude Area Defense
TT&M	Targeting, Tracking, and Measurement
UAS	Unmanned Aerial Systems
UAV	Unmanned Aerial Vehicle
UHF	Ultra-High Frequency
USAF	U.S. Air Force
USSR	Union of Soviet Socialist Republics
VSAT	Very Small Aperture Terminal

EXECUTIVE SUMMARY

The space domain is undergoing a significant set of changes. A growing number of countries and commercial actors are getting involved in space, resulting in more innovation and benefits on Earth, but also more congestion and competition in space. From a security perspective, an increasing number of countries are looking to use space to enhance their military capabilities and national security. The growing use of, and reliance on, space for national security has also led more countries to look at developing their own counterspace capabilities that can be used to deceive, disrupt, deny, degrade, or destroy space systems.

The existence of counterspace capabilities is not new, but the circumstances surrounding them are. Today there are increased incentives for development, and potential use, of offensive counterspace capabilities. There are also greater potential consequences from their widespread use that could have global repercussions well beyond the military, as huge parts of the global economy and society are increasing reliant on space applications.

This report compiles and assesses publicly-available information on the counterspace capabilities being developed by multiple countries across five categories: direct-ascent, co-orbital, electronic warfare, directed energy, and cyber. It assesses the current and near-term future capabilities for each country, along with their potential military utility. The evidence shows significant research and development of a broad range of kinetic (i.e. destructive) and non-kinetic counterspace capabilities in multiple countries. **However, only non-kinetic capabilities are actively being used in current military operations.** The following provides a more detailed summary of each country's capabilities.

China

The evidence strongly indicates that China has a sustained effort to develop a broad range of counterspace capabilities. China has conducted multiple tests of technologies for close approach and rendezvous in both low-earth orbit (LEO) and geosynchronous orbit (GEO) that could lead to a co-orbital ASAT capability. However, as of yet, the public evidence indicates they have not conducted an actual destructive intercept of a target, and there is no proof that these RPO technologies are definitively being developed for counterspace use as opposed to intelligence gathering or other purposes.

China has at least one, and possibly as many as three, programs underway to develop direct ascent anti-satellite (DA-ASAT) capabilities, either as dedicated counterspace systems or as midcourse missile defense systems that could provide counterspace capabilities. China has engaged in multiple, progressive tests of these capabilities since 2005, indicating a serious organizational effort. Chinese DA-ASAT capability against LEO targets is likely mature and may be operationally fielded on mobile launchers within the next few years. Chinese DA-ASAT capability against deep space targets - both medium Earth Orbit (MEO) and GEO - is likely still in the

experimental or development phase, and there is not sufficient evidence to conclude whether it will become an operational capability in the near future.

Although official Chinese statements on space warfare and weapons have remained consistently aligned to the peaceful purposes of outer space, privately they have become more nuanced. China has recently designated space as a military domain, and military writings state that the goal of space warfare and operations is to achieve space superiority using offensive and defensive means in connection with their broader strategic focus on asymmetric cost imposition, access denial, and information dominance. That said, it is uncertain whether China would fully utilize its offensive counterspace capabilities in a future conflict or whether the goal is to use them as a deterrent against U.S. aggression. There is no public evidence of China actively using counterspace capabilities in current military operations.

Russia

There is strong evidence that Russia has embarked on a set of programs over the last decade to regain some of its Cold War-era counterspace capability. Since 2010, Russia has been testing technologies for close approach and rendezvous in both LEO and GEO that could lead to a co-orbital ASAT capability, and some of those efforts have links to a Cold War-era LEO co-orbital ASAT program. However, the technologies could also be used for non-aggressive applications, and the on-orbit testing done to date does not conclusively prove they are for an ASAT program.

Russia is almost certainly capable of some limited DA-ASAT operations, but likely not yet on a sufficient scale or at sufficient altitude to pose a critical threat to U.S. space assets. Core Russian direct-ascent ASAT capabilities are not yet operational, and those currently in development are not planned to have the capability to threaten targets beyond LEO. Russia appears highly motivated to continue development efforts even where military utility is questionable, due at least in part to bureaucratic pressures.

Russia places a high priority on integrating electronic warfare (EW) into military operations and has been investing heavily in modernizing this capability. Most of the upgrades have focused on multifunction tactical systems whose counterspace capability is limited to jamming of user terminals within tactical ranges. Russia has a multitude of systems that can jam GPS receivers within a local area, potentially interfering with the guidance systems of unmanned aerial vehicles (UAVs), guided missiles, and precision guided munitions, but has no publicly known capability to interfere with the GPS satellites themselves using radiofrequency interference. The Russian Army fields several types of mobile EW systems, some of which can jam specific satellite communications user terminals within tactical ranges. Russia can likely jam communications satellites uplinks over a wide area from fixed ground stations facilities. Russia has operational experience in the use of counterspace EW capabilities from recent military campaigns.

Russia has a strong technological knowledge base in directed energy physics and is developing a number of military applications for laser systems in a variety of environments. Russia has revived,

and continues to evolve, a legacy program whose goal is develop an aircraft-borne laser system for targeting the optical sensors of imagery reconnaissance satellites, although there is no indication that an operational capability has been yet achieved. Although not their intended purpose, Russian ground-based satellite laser ranging (SLR) facilities could be used to dazzle the sensors of optical imagery satellites. There is no indication that Russia is developing, or intending to develop, high power space-based laser weapons.

Russian military thinkers see modern warfare as a struggle over information dominance and net-centric operations that can often take place in domains without clear boundaries and contiguous operating areas. To meet the challenge posed by the space-aspect of modern warfare, Russia is pursuing lofty goals of incorporating EW capabilities throughout its military to both protect its own space-enabled capabilities and degrade or deny those capabilities to its adversary. In space, Russia is seeking to mitigate the superiority of U.S. space assets by fielding a number of ground, air, and space-based offensive capabilities. Although technical challenges remain, the Russian leadership has indicated that Russia will continue to seek parity with the United States in space.

The United States

The United States has conducted multiple tests of technologies for close approach and rendezvous in both LEO and GEO, along with tracking, targeting, and intercept technologies that could lead to a co-orbital ASAT capability. These tests and demonstrations were conducted for other non-offensive missions, such as missile defense, on-orbit inspections, and satellite servicing, and the United States does not have an acknowledged program to develop co-orbital capabilities. However, the United States possesses the technological capability to develop a co-orbital capability in a short period of time if it chooses to.

While the United States does not have an operational, acknowledged DA-ASAT capability, it does have operational midcourse missile defense interceptors that have been demonstrated in an ASAT role against low LEO satellites. The United States has developed dedicated DA-ASATs in the past, both conventional and nuclear-tipped, and likely possesses the ability to do so in the near future should it choose so.

The United States has an operational EW counterspace system, the Counter Communications System (CCS), which can be deployed globally to provide uplink jamming capability against geostationary communications satellites. The United States likely has the capability to jam global navigation satellite service receivers (GPS, GLONASS, Beidou) within a local area of operation to prevent their effective use by adversaries. In addition to interfering with adversarial use of satellite navigation, the Navigation Warfare program seeks to assure the availability of GPS services for U.S. military units in operations. The effectiveness of measures to counter adversarial GPS jamming and spoofing operations is not known.

The United States has had established doctrine and policy on counterspace capabilities for several decades, although not always publicly expressed. Most U.S. presidential administrations since the

1960s have directed or authorized research and development of counterspace capabilities, and in some cases greenlit testing or operational deployment of counterspace systems. These capabilities have typically been limited in scope, and designed to counter a specific military threat, rather than be used as a broad coercive or deterrent threat. The U.S. military doctrine for space control includes defensive space control (DSC), offensive space control (OSC), and is supported by space situational awareness (SSA).

Since 2014, U.S. policymakers have placed increased focus on space security, and have increasingly talked publicly about preparing for a potential "war in space", speaking openly about space being a warfighting domain. This rhetoric has been accompanied by a renewed focus on reorganizing national security space structures and increasing the resilience of space systems. It is possible that the United States has also begun development of new offensive counterspace capabilities, although there is no publicly-available policy or budget direction to do so. The United States also continues to hold annual space wargames and exercises that increasingly involve close allies and commercial partners.

Iran

Iran has a nascent space program, building and launching small satellites that have limited capability. Technologically, it unlikely Iran has the capacity to build on-orbit or direct-ascent anti-satellite capabilities, and little military motivations to do so at this point. Iran has demonstrated an EW capability to persistently interfere with commercial satellite signals, although the capability against military signals is difficult to ascertain.

North Korea

North Korea has no demonstrated capability to mount kinetic attacks on U.S. space assets: neither a direct ascent ASAT nor a co-orbital system. In its official statements, North Korea has never mentioned anti-satellite operations or intent, suggesting that there is no clear doctrine in Pyongyang's thinking at this point. North Korea does not appear motivated to develop dedicated counterspace assets, though certain capabilities in their ballistic missile program might be eventually evolved for such a purpose. It is unlikely that North Korea would use one of its few nuclear weapons as an electromagnetic weapon.

North Korea has demonstrated the capability to jam civilian GPS signals within a limited geographical area. Their capability against U.S. military GPS signals is not known. There has been no demonstrated ability of North Korea to interfere with satellite communications, although their technical capability remains unknown.

India

India has over five decades of experience with space capabilities, but most of that has been civil in focus. It is only in the past several years that India has started organizationally making way for its military to become active users and creators of its space capabilities. India's military has been

developing an indigenous missile defense program that its supporters argue could provide a latent ASAT capability, should the need arise; this capability has not been tested. It is possible that India would move into rapidly testing an ASAT if it felt that the international community was getting close to creating an international legal regime banning kinetic ASAT tests; otherwise, given the substantial investment the Indian military is making in its satellite capacity and the income that India is receiving from launching other countries' satellites, it is unlikely that they will move to actively create an official counterspace program.

Cyber Capabilities

Multiple counties possess cyber capabilities that could be used against space systems; however actual evidence of cyber attacks in the public domain are limited. The United States, Russia, China, North Korea, and Iran have all demonstrated the ability and willingness to engage in offensive cyber attacks against non-space targets. Additionally, a growing number of non-state actors are actively probing commercial satellite systems and discovering cyber vulnerabilities that are similar in nature to those found in non-space systems. This indicates that manufacturers and developers of space systems may not yet have reached the same level of cyber hardness as other sectors.

There is a clear trend toward lower barriers to access, and widespread vulnerabilities coupled with reliance on relatively unsecured commercial space systems create the potential for non-state actors to carry out some counter-space cyber operations without nation-state assistance. However, while this threat deserves attention and will likely grow in severity over the next decade, there remains a stark difference at present between the cyber attacks capabilities of leading nation-states and other actors.

ACKNOWLEDGEMENTS

This publication would not have been possible without the contributions from the following individuals who contributed their time and expertise in a personal capacity. We are deeply grateful for their expertise and commitment.

Catherine Dill
Gilles Doucet
Jeffrey Edmonds
Laura Grego
Brandon Kelley
Jonathan McDowell
Sean O'Connor
Pavel Podvig
Kevin Pollpeter
Josh Wolny

This work is a synthesis of all these individual contributions with those from SWF staff, and as such Secure World Foundation bears all responsibility for any errors or omissions.

We also would like to thank Planet for kindly providing access to their imagery database through their Planet Explorer program.

FOREWORD

Space security has become an increasingly salient policy issue. Over the last several years, there has been growing concern from multiple governments over the reliance on vulnerable space capabilities for national security, and the corresponding proliferation of offensive counterspace capabilities that could be used to disrupt, deny, degrade, or destroy space systems. This in turn has led to increased rhetoric from some countries about the need to prepare for future conflicts on Earth to extend into space and calls from some corners to increase the development of offensive counterspace capabilities and put in place more aggressive policies and postures.

Unfortunately, much of this debate has taken place out of sight of the public, largely due to the reluctance of most countries to talk openly about the subject. Part of this can be traced to the classified nature of the intelligence on offensive counterspace capabilities and to the unwillingness to reveal details that could compromise sources and methods. But part of it is also the political sensitivity of the topic, and the discrepancies between what countries say in public and what they may be doing behind the scenes. At the same time, some media outlets and pundits have used what little information is known to make hyperbolic claims that do not add constructively to the debate.

We feel strongly that a more open and public debate on these issues is urgently needed. Space is not the sole domain of militaries and intelligence services. Our global society and economy is increasingly dependent on space capabilities, and a future conflict in space could have massive, long-term negative repercussions that are felt right here on Earth. The public should be as aware of the developing threats and risks of different policy options as would be the case for other national security issues in the air, land, and sea domains.

The purpose of the project was to provide a public assessment of counterspace capabilities being developed by countries based on unclassified information. We hope doing so will increase public knowledge of these issues, the willingness of policymakers to discuss these issues openly, and involvement of other stakeholders in the debate.

Finally, we must note that this publication is not meant to be the conclusive answer on these issues. We have done our best to base our findings and assessments on publicly-available data, and we would like to thank our expert contributors for their hard work on this issue. However, some of the topics discussed here are difficult to assess using open sources, and we acknowledge that significant gaps are likely to remain. Our limited resources also prevented us from covering all the topics we had hoped to in this first edition. We intend to publish future editions of this publication that address these shortcomings, and continually work with the broader space community to improve this assessment.

Brian Weeden and Victoria Samson

INTRODUCTION

The space domain is undergoing a significant set of changes. A growing number of countries and commercial actors are getting involved in space, resulting in more innovation and benefits on Earth but also more congestion and competition in space. From a security perspective, an increasing number of countries are looking to use space to enhance their military capabilities and national security. Most of the space applications they are developing are not new and have been developed by the United States or the Soviet Union since the beginning of the Space Age. Space-based, intelligence, surveillance, reconnaissance (ISR), positioning navigation and timing (PNT), and satellite communications (SATCOM) are staples of military space applications. What has changed is the proliferation of these capabilities beyond just superpowers.

The growing use of, and reliance on, space for national security has also led more countries to look at developing their own counterspace capabilities. **Counterspace**, also known as **space control**, is the set of capabilities or techniques that are used to gain space superiority. **Space superiority** is the ability to use space for one's own purposes while denying it to an adversary. Accordingly, counterspace capabilities have both offensive and defensive elements, which are both supported by **space situational awareness** (information about the space environment). Defensive counterspace helps protect one's own space assets from attack, while offensive counterspace tries to prevent the adversary from using their space assets. Antisatellite (ASAT) weapons are a subset of offensive counterspace capabilities, although the satellite itself is only one part of the system that can be attacked. Offensive capabilities can be used to deceive, disrupt, deny, degrade, or destroy any of the three elements of a space system: the satellite, the ground system, or the communication links between them.

A key driver in the proliferation of offensive counterspace capabilities is the increased use of space in conventional warfare. For much of the Cold War, space was limited to mainly a strategic role in collecting strategic intelligence, enforcing arms control treaties, and warning of potential nuclear attack. And although the Cold War saw significant development and testing of counterspace capabilities, the close link between space capabilities and nuclear war provided a level of deterrence against actual attacks on space systems. But over the last two decades, many of these strategic space capabilities have found new roles in directly supporting conventional wars by providing operational and tactical benefits to militaries. This has increased the incentives for countries to develop offensive counterspace capabilities, while also decreasing the deterrent value of the nuclear link.

While there are undeniable military benefits to these new uses of space, there are risks as well. First, the growing reliance on space for national security and the proliferation of counterspace capabilities creates an increased risk that incidents in space can spark or escalate conflict on Earth. The sudden loss or interruption of space capabilities during a period of heightened geopolitical tensions could create the assumption that it is the opening salvo of an armed attack, even if it was a natural event or an onboard failure. Second, actual use of offensive counterspace capabilities

could have long-lasting consequences for humanity, whether through the loss of critical space capabilities that underpin the global economy and societies or through the creation of long-lived space debris that hinders future space activities.

To help address this issue, Secure World Foundation began a project in the summer of 2017 to develop an open source assessment of global counterspace capabilities. We convened a group of international experts to work with our staff to compile publicly-available information on global development of counterspace capabilities across several countries. We looked at several distinct categories of offensive counterspace capabilities:

- **Direct Ascent**: weapons that use ground, air-, or sea-launched missiles with interceptors that are used to kinetically destroy satellites through force of impact, but are not placed into orbit themselves
- **Co-orbital**: weapons that are placed into orbit and then maneuver to approach the target
- **Directed Energy**: weapons that use focused energy, such as laser, particle, or microwave beams to interfere or destroy space systems
- **Electronic Warfare**: weapons that use radiofrequency energy to interfere with or jam the communications to or from satellites
- **Cyber**: weapons that use software and network techniques to compromise, control, interfere, or destroy computer systems

For each of these categories, we assessed what the current and near-term capabilities might be for the countries examined in this report, based on the publicly-available information. We also assessed the potential military utility for each capability, which includes both the advantages and disadvantages of the capabilities. Finally, when possible, we also examined each country's policy, doctrine, and budget to support the offensive counterspace capabilities being developed. Taken together, this analysis is intended to provide a more holistic picture of what each country is working on, and how these capabilities may be used.

The countries we chose to examine in this report are the ones most active in developing their own indigenous offensive counterspace capabilities. However, they should not be taken as an exhaustive list of countries doing so. Some of the capabilities, such as jamming, are difficult to observe while in development, and may be much more widely proliferated than indicated here. It is likely, however, that the types of counterspace capabilities being developed by other countries are similar to those discussed in this report.

Many of the details contained in this report will not be new to the government experts who have been analyzing these same trends. In fact, we hope that much of our work replicates theirs. However, since much of the government work on these issues is classified or otherwise not divulged to the public, the assessment presented in this report is likely to be new to those who do not have active security clearances. We hope that it provides useful context to the soundbites and

headlines being generated over military and political leaders' concern about counterspace and space superiority.

Finally, while we have strived to make this report as unbiased and accurate as possible, like all analytical products, it should be read with a degree of skepticism. A significant degree of judgment was used in determining which sources of information to include in this report, and how to weigh their impact on the overall assessment. Many of the sources themselves are flawed in that they originate from media reports that similarly are the product of individual judgment about what to report, or not to report. Wherever possible, we tried to include the lowest level of reference for the information presented here so that the reader can bring their own judgment to bear.

Much debate went into how to organize the information presented in this report. On the one hand, it could be organized by capability with sub-sections for developments in each country, which would emphasize the similarities or differences in how each country was developing related technologies. On the other hand, it could be organized by country with sub-sections for developments in each capability, which would give a better picture of each country's overall counterspace effort. The quantity of information varied significantly between countries, and some capabilities, such as cyber, were difficult to break down by specific countries due to a paucity of publicly-available data.

Ultimately, we chose to organize the following chapters primarily by country and then capability. For China, Russia, and the United States, each category of capability is given its own sub-section due to the significant amount of history and activity. For the other countries, a single integrated chapter is presented. There is also a dedicated chapter for cyber that integrates capabilities being developed across all countries. At the end is an Appendix which includes imagery of major testing sites and facilities discussed in the report.

1 – PEOPLE'S REPUBLIC OF CHINA

Over the last few decades, China has embarked on a sustained national effort to develop a broad spectrum of space capabilities across the civil, national security, and commercial sectors. Space capabilities under development by China include a robust human spaceflight and robotic space exploration program; remote sensing for weather and resource management; and military applications such as positioning, navigation and timing and intelligence, surveillance and reconnaissance.

China appears to be highly motivated to develop counterspace capabilities in order to bolster its national security. China is beginning to more strongly assert its regional political, economic, and military interests, and sees counterspace capabilities as a key enabler. Much has been written about how reliant the United States is on space capabilities to project global military power, and thus being able to counter U.S. space capabilities is a key element of China's ability to assure its freedom of action and deter potential U.S. military operations in its sphere of influence.

There is strong evidence suggesting that China has a sustained effort to develop a broad range of counterspace capabilities. Over the last decade, China has engaged in multiple tests of technologies and capabilities that either are offensive counterspace weapons or could be used as such. China has also begun developing the policy, doctrine, and organizational frameworks to support the integration of counterspace capabilities into its military planning and operations. That said, it is unclear whether China intends to fully utilize counterspace capabilities in a future conflict, or whether the goal is to use them as a deterrent against aggression. There is no public evidence of China actively using counterspace capabilities in current military operations.

The following sections provide details on China's development of co-orbital and direct ascent capabilities, and the policy and doctrine framework to support those capabilities. It is likely China is also developing, or may already possess, significant directed energy and electronic warfare counterspace capabilities as well. However, we chose not to include them in this report at this time due to the challenges in obtaining trustworthy open source information on those activities.

1.1 - Chinese Co-Orbital ASAT

Assessment

China has conducted multiple tests of technologies for close approach and rendezvous in both low-earth orbit (LEO) and geostationary earth orbit (GEO) that could lead to a co-orbital ASAT capability. However, as of yet, the public evidence indicates they have not conducted an actual destructive intercept of a target, and there is no proof that these technologies are definitively being developed for counterspace use as opposed to intelligence gathering or other purposes.

Specifics

China has conducted a series of on-orbit demonstrations of rendezvous between different pairs of unmanned satellites. The first known incident occurred in LEO in the summer of 2010[1] and involved the Chinese satellites Shi Jian 12 (SJ-12, International designator 2010-027A, U.S. catalog number 36596), and the SJ-06F (2008-053B, 33409). The SJ-06F was launched on October 25, 2008,[2] and the SJ-12 was launched on June 15, 2010. Both satellites were reportedly built by the Shanghai Academy of Spaceflight Technology (SAST) under contract to the China Aerospace Science and Technology Corporation (CASC). The official mission for the SJ-06 series satellites is to measure the space environment and perform space experiments. Some observers believe that their true mission is collection of electronic intelligence (ELINT) or signals for the Chinese military, in part because no scientific research is known to have been published based on the work of these satellites.[3] The mission of SJ-12, as stated by the State media service Xinhua, is to carry out "scientific and technological experiments, including space environment probe [sic], measurement, and communications."[4] Both the SJ-12 and SJ-06F were in orbits between 600 kilometers (km) and 570 km sun-synchronous orbits with an inclination of 97.6 degrees.

In the summer of 2010, the SJ-12 initiated a series of deliberate changes in its orbital trajectory to approach and rendezvous with the SJ-06F satellite.[5] The maneuvers occurred over several weeks between June 12, 2010, and August 16, 2010, and indicated a very slow and methodical approach. On August 19, the two satellites had their closest approach, which was estimated to be less than 300 meters (m). A change in the orbital trajectory for the SJ-06F around that same time indicates that the two satellites may have bumped into each other, although at a very slow relative speed of a few meters per second. There were no external indications of damage to either satellite, nor any

[1] A previous incident in October 2008 involving the Chinese BX-1 microsatellite and the International Space Station was most likely an incidental conjunction, as the BX-1 was not under any active control at the time. For more details, see 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.
[2] Mark Wade, "SJ-6," *Astronautix,* accessed March 22, 2018, http://www.astronautix.com/s/sj-6.html.
[3] Ibid.
[4] Leiying Xu, "China Sends Research Satellite into Space," *Xinhua*, updated June 15, 2010. http://english.cri.cn/6909/2010/06/15/1821s576844.htm.
[5] A more detailed technical analysis of this event can be found in Brian Weeden, "Dancing in the Dark; The Orbital Rendezvous of SJ-12 and SJ06F," *The Space Review*, August 30, 2010, http://www.thespacereview.com/article/1689/1.

debris created by the incident. The incident appears to have been similar to the bumping that occurred during the autonomous rendezvous attempt between NASA's Demonstration for Autonomous Rendezvous Technology (DART) satellite and the U.S. Navy's Multiple Path Beyond Line of Site Communication (MUBLCOM) satellite in April 2005 (See U.S. Co-Orbital ASAT; section 3-2).[6]

Another rendezvous between two Chinese satellites in LEO occurred in 2013. On July 19, 2013, China placed three payloads into orbit into roughly similar orbits around 670 km altitude and 98 degrees inclination. the same launch: Shiyan 7 (SY-7), Chuangxin 3 (CX-3), and Shijian 15 (SJ-15). The mission was publicly described by the Chinese government as "conducting scientific experiments on space maintenance technologies."[7] Public information at the time indicated the SY-7 was built by the DFH Satellite Corporation on behalf of the Chinese Academy of Space Technology (CAST), and likely carried a robotic arm being developed to support China's space station program, perhaps similar to the Canadian robotic arm used on the International Space Station.[8] SJ-15 was built by the SAST after eight years of development, and was reportedly an optical space tracking satellite similar to the U.S. Air Force's Space-Based Surveillance System (SBSS) satellite.[9] CX-3 was built by the Chinese Academy of Sciences, and was likely a small store-and-forward communications satellite that was the most recent in a series of such satellites.[10] Once on orbit, the three satellites were cataloged as Payload A (2013-037A, 39208), Payload B (2013-037B, 39209), and Payload C (2013-037C, 39210) by the U.S. military.[11]

In August 2013, Payload C initiated a series of maneuvers to alter its orbit and bring it close to two other satellites. On August 9, Payload C altered its altitude by a few tens of kilometers, which meant it passed above Payload B at a distance of a few kilometers before returning largely to its original orbit. On August 16, Payload C altered its altitude by more than 100 km and its inclination by 0.3 degrees, which eventually led to a close approach of Shi Jian 7 (SJ-7), a Chinese satellite launched in 2005 (2005-024A, 28737), to within a few kilometers.[12] Anonymous U.S. officials claimed that the rendezvous was part of a "covert anti-satellite weapons development program,"

[6] "Overview of the DART Mishap Investigation Results," NASA, accessed March 22, 2018. http://www.nasa.gov/pdf/148072main_DART_mishap_overview.pdf.
[7] Jonathan McDowell, posting on the NASAspaceflight.com forums, July 20, 2013, http://forum.nasaspaceflight.com/index.php?topic=30486.msg1076481#msg1076481.
[8] Posting on the 9ifly.cn Forums, August 8, 2013, http://bbs.9ifly.cn/forum.php?mod=viewthread&tid=9551&page=1#pid261125.
[9] Posting on the 9ifly.cn Forums, July 26, 2013, http://bbs.9ifly.cn/forum.php?mod=viewthread&tid=10910&page=16#pid259544.
[10] Gunter Krebs, "CX 1," *Gunter's Space Page*, updated November 12, 2017, http://space.skyrocket.de/doc_sdat/cx-1.htm.
[11] Due to the uncertainty regarding which payload was which, the public Space Track catalog has not identified which satellite was which. They are still labeled Payload A, Payload B, and Payload C.
[12] Marcia Smith, "Surprise Chinese satellite maneuvers mystify western experts," *Space Policy Online*, updated August 19, 2013, http://spacepolicyonline.com/news/surprise-chinese-satelllite-maneuvers-mystify-western-experts/.

and that one of the satellites "grabbed" another,[13] although there's no way to confirm a physical docking from the publicly-available tracking data.

On October 18, 2013, Payload A initiated a small maneuver to raise its orbit by several hundred meters, and shortly thereafter released another object, which the U.S. military labeled Payload A Debris (2013-037J, 39357). Payload A and Payload A debris orbited in relatively close proximity to each other for several days, ranging between a few kilometers and several hundred meters, with some reports claiming the two objects may have physically joined with each other.[14] However, the publicly-available tracking is not accurate enough to confirm those claims. Both objects occasionally conducted small maneuvers throughout 2014 and 2015, although the separation distance between them never exceeded more than a few kilometers.

In April 2014, Payload C began another series of small maneuvers to once again conduct proximity operations around Payload B. Between April 12-14, Payload C raised its orbit by several tens of kilometers, and then between May 12 and 14, Payload C lowered its orbit by several tens of kilometers. The effect of these maneuvers was to once again match orbital planes with the SJ-7, and on a trajectory that brought it above and then behind the SJ-7 at a range of around 150 km, with a vertical separation of a few kilometers.[15] Over the course of the rest of May, Payload C slowly decreased the distance to the SJ-7 to within a kilometer.[16]

A year later, in October 2014, an internet code repository was discovered that supported earlier claims that the three satellites were engaged in capture and surveillance activities. Payload A was known internally to the Chinese program as Tansuo-4, corresponding to the public designation SY-7, and was designed with a teleoperated robotic arm that interacted with the separating subsatellite, as shown at the lower left of Figure 1 below. Payload B was known internally as Tansuo-3, corresponding to the public designation CX-3, and was designed to provide optical surveillance of space objects in geostationary and low Earth orbits. Payload C was known internally as Tansuo-5, corresponding to the SJ-15, and was designed to maneuver and conduct proximity operations with other space objects.

[13] Bill Gertz, "China Testing New Space Weapons," *The Washington Free Beacon*, October 2, 2013, http://freebeacon.com/national-security/china-testing-new-space-weapons/.
[14] Marcia Smith, "Did China Succeed in Capturing One of its own Satellites? – Update," *Space Policy Online*, updated October 26, 2013, http://spacepolicyonline.com/news/did-china-succeed-in-capturing-one-of-its-own-satellites/.
[15] Posting on Novosti Kosmonavtiki forums, May 5, 2014, http://novosti-kosmonavtiki.ru/forum/messages/forum12/topic13702/message1254275/#message1254275.
[16] Posting on Novosti Kosmonavtiki forums, May 29, 2014, http://novosti-kosmonavtiki.ru/forum/messages/forum12/topic13702/message1262548/#message1262548.

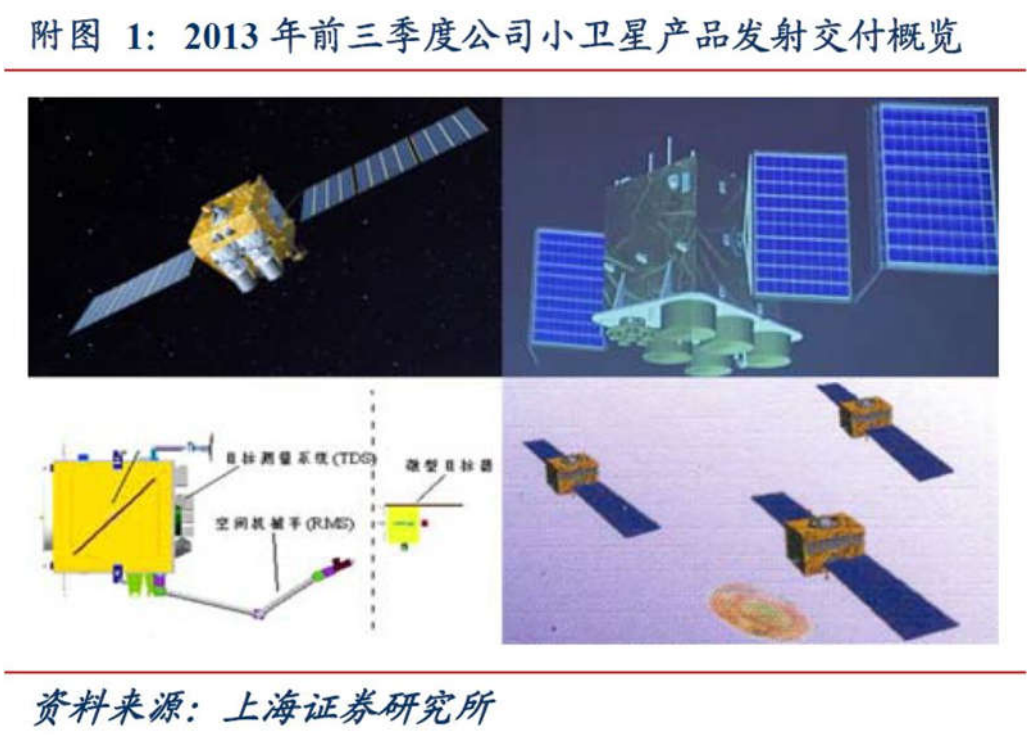

Figure 1 - Co-Orbital SJ-7
Image of the SJ-7 (lower left, with robotic arm) and its small companion satellite.
Image credit: Liss[17]

Payload C continued to occasionally make changes to its orbit in 2015 and 2016, but the reasons for doing so were unclear. On December 3, 2015, Payload C increased its inclination by 0.3 back to 98 degrees. On May 6, 2016, Payload C changed its altitude by several tens of kilometers to once again bring it close to Payload B.[18]

In 2016, another Chinese satellite was launched that again created concerns about on-orbit grappling. The Aolong-1 (AL-1), also known as the Advanced Debris Removal Vehicle (ADRV) or "Roaming Dragon," was a small satellite developed by Harbin Institute of Technology under contract to CALT to reportedly demonstrate using a robotic arm to capture a small piece of space debris for removal from orbit. Aolong-1 was placed into orbit on the first launch of China's new Long March 7 (LM-7) rocket on June 25, 2016, along with a scaled-down test version of China's next human spacecraft, a ballast mass, and a few small rideshare cubesats. The purpose of the launch was to demonstrate the ability of the LM-7 and its restartable upper stage to place the new crewed spacecraft into orbit, to deploy multiple payloads into different orbits, test the new

[17] Posting on Novosti Kosmonavtiki forums, January 1, 2016, http://novosti-kosmonavtiki.ru/forum/messages/forum12/topic13702/message1462007/#message1462007.
[18] Posting on NASAspaceflight.com forums, June 7, 2016, http://forum.nasaspaceflight.com/index.php?PHPSESSID=iamdpaq7ig407ooqdmi8gm06k6&topic=30486.msg1545873#msg1545873.

Tianyuan-1 refueling system developed by the National University of Defense Technology, and test the atmospheric re-entry of the crewed spacecraft test vehicle.[19]

Although they were only small parts of the mission, the debris removal and refueling experiments generated significant press outside of China due to concerns over dual-use technology and China leaping ahead in technology. Stories included an inflammatory report that quoted a researcher from the National Astronomical Observatories in Beijing talking about the potential for Aolong-1 to be used as a weapon system.[20] However, it is unclear whether the researcher was truly convinced that was indeed the motive for Aolong-1, or whether he was hypothesizing about military applications for debris removal technology in general, much as American scientists and officials often do.[21] More media stories were generated that claimed the same test had included the successful refueling of another satellite,[22] and that the two events taken together demonstrated China's increasing technological prowess.[23]

The reality of either the Aolong-1 or the refueling experiment was less than the media hype. By all appearances, the Tianyuan-1 refueling system was attached to the upper stage, as no separate satellite of that description was ever cataloged by the U.S. military, nor did any of the ten objects cataloged in space rendezvous with any other satellites. According to U.S. military tracking data, the Aolong-1 did indeed separate into a 380 km by 200 km orbit but did not rendezvous with any other objects. The debris capture experiment appears to have been simulated, and the Aolong-1 does not appear to have altered its orbit during its short two months on orbit.[24]

Another incident of rendezvous and proximity operations (RPO) between two Chinese satellites occurred in 2016, but this time in GEO. On November 3, 2016, China lofted the SJ-17 satellite to GEO on the maiden launch of its new Long March 5 (LM-5) space launch vehicle. The SJ-17 was reportedly designed to test advanced technologies such as environmentally-friendly chemical propellant, ion propulsion, quad-junction gallium arsenide solar panels, and an on-board optical

[19] "China lands Prototype Crew Spacecraft after inaugural Long March 7 Launch," *Spaceflight101*, June 27, 2016, http://spaceflight101.com/long-march-7-maiden-launch/china-lands-prototype-crew-spacecraft-after-inaugural-long-march-7-launch/.
[20] "Is China militarising space? Experts say new junk collector could be used as anti-satellite weapon," *South China Morning Post*, updated June 12, 2017, http://www.scmp.com/news/china/diplomacy-defence/article/1982526/china-militarising-space-experts-say-new-junk-collector.
[21] During a 2011 workshop organized by the National Research Council as part of a study of NASA's space debris program, participants stated that a Department of Defense plan to remove space debris did not go forward in part due to concerns that "most of the proposals had a weapons-like character about them". See National Research Council, *Limiting Future Collision Risk to Spacecraft: An Assessment of NASA's Meteoroid and Orbital Debris Programs*, Washington, DC: National Academies Press, 2011, https://doi.org/10.17226/13244, pg. 143.
[22] Jon Fingas, "China successfully refuels a satellite in orbit," *Engadget*, July 2, 2016, https://www.engadget.com/2016/07/02/china-refuels-satellite-in-orbit/.
[23] Jeffrey Lin and P.W. Singer, "China's largest space launch vehicle, the Long March 7 flies, with a Technological Triple Whammy," *Popular Science*, July 8, 2016, http://www.popsci.com/chinas-largest-space-launch-vehicle-long-march-7-flies-with-technological-triple-whammy.
[24] "Re-Entry: Aolong-1 Space Debris Removal Demonstrator," *Spaceflight101*, August 28, 2016, http://spaceflight101.com/re-entry-aolong-1-space-debris-removal-demonstrator/

surveillance sensor.[25] The launch was typical of the historical process of getting most satellites to GEO using chemical propulsion,[26] taking about 6 hours and 14 minutes after launch.[27] The only anomaly was with the Yuanzheng-2 (YZ-2) upper stage that carried the SJ-17 to GEO. The YZ-2 failed to do a disposal maneuver to remove itself from the protected GEO zone in accordance with international debris mitigation guidelines. Instead, the YZ-2 remained in an orbit with a perigee near GEO altitude such that the YZ-2 will occasionally dip down very close to, and rotate around, the active GEO belt for decades to come.

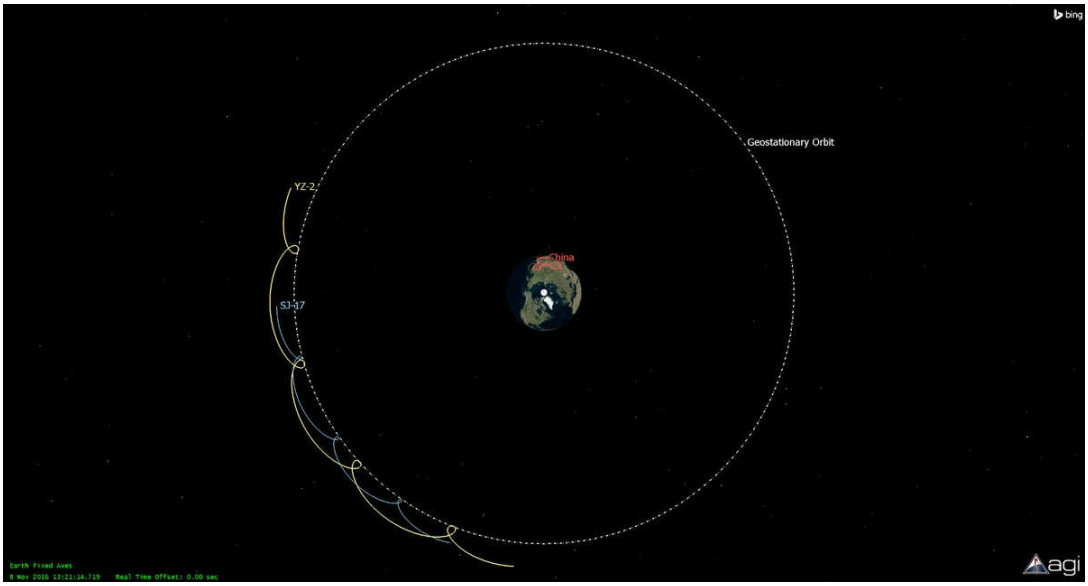

Figure 2 - Orbital trajectory of the YZ-2
Simulation of the upper stage as it periodically intrudes on the active GEO belt.
Image credit: AGI.[28]

Several days after reaching GEO and separating from the YZ-2, the SJ-17 began maneuvering to place itself into the active GEO belt close to another Chinese satellite. It began with a maneuver on November 10 to lower its orbit and reduce its westward drift, and then a pair of maneuvers on November 11 to fully stabilize within the active GEO belt at a longitude of 162.9 E. This placed the SJ-17 relatively close to another Chinese satellite, Chinasat 5A (1998-033A, 25354).[29] Chinasat 5A was originally built by Lockheed Martin under contract to the Chinese Communications Ministry, and launched in 1998 under the name Zongwei 1 to provide

[25] "China's Shijian-17 Satellite settles in Geostationary Orbit for Experimental Mission," *Spaceflight101*, November 24, 2016, http://spaceflight101.com/shijian-17-settles-in-geostationary-orbit/.
[26] The other major method of getting to GEO utilizes constant thrust ion propulsion, which can take weeks or months.
[27] "China's Shijian-17 Satellite settles in Geostationary Orbit for Experimental Mission," *Spaceflight101*, November 24, 2016, http://spaceflight101.com/cz-5-maiden-flight/shijian-17-settles-in-geostationary-orbit/.
[28] Analytical Graphics (@AGItweets), "Here's what #ComSpOC's been tracking for YZ-2 and SJ-17 as of Nov 7th. Both drifting at 20+ degrees/day #LongMarch5," Tweet, November 8, 2016, https://twitter.com/i/web/status/796026741911392257.
[29] Originally, this was reported as Chinasat 6A closing in with Chinasat 5A, due to the U.S. military mislabeling the SJ-17 as Chinasat 6A.

commercial satellite communications services for southeast Asia.[30] The SJ-17 made several small maneuvers to circumnavigate Chinasat 5A at a distance of between 100 and 50 km for several days, slowly closing in to within a few km on November 30, and then returning to a 100 to 50 km standoff distance.[31] The two satellite remained close until December 29, when AGI reported that Chinasat 5A had begun drifting away.[32]

On April 26, 2017, the SJ-17 began drifting again, and stopped around the end of June at 125 E. It drifted again between September 29 and October 10, 2017, settling in at 118 E. On January 11, 2018, the SJ-17 began a rapid eastward drift at two degrees per day, followed by a rapid drift westward at four degrees per day starting on February 9. On March 20, the SJ-17 lowered its orbit to reverse its drift, indicating that it is doing fast survey of the GEO region.

The activities of the SJ-12, SJ-15, and SJ-17 are consistent with the demonstration of RPO technologies for the purpose of satellite servicing and inspection. Specifically, they appear similar in nature to the activities of the U.S. Air Force's XSS-11 satellite, which was used to do inspections of satellites in LEO in 2005 and 2006;[33] DARPA's OrbitalExpress satellite, which launched as a joined pair and conducted a series of rendezvous, docking, and robotic arm experiments in 2007;[34] the Swedish Mango and Tango cubesats that were part of the Prototype Research Instruments and Space Mission technology Advancement (PRISMA) mission, which demonstrated cooperative rendezvous and proximity operations and formation flying in 2010;[35] and the U.S. Air Force's Micro-satellite Technology Experiment (MiTEx) satellites[36] and Geostationary Space Situational Awareness (GSSAP) satellites,[37] which conducted inspections in the GEO belt in 2009 and 2016, respectively (See U.S. Co-Orbital ASAT; Section 3-2).

[30] Gunter Krebs, "Zhongwei 1 (ChinaStar 1) → ZX 5A (ChinaSat 5A) → APStar 9A," *Gunter's Space Page*, updated November 12, 2017, http://space.skyrocket.de/doc_sdat/zhongwei-1.htm.
[31] "In-Space Eavesdropping? – China's Shijian-17 completes High-Altitude Link-Up," *Spaceflight101* December 9, 2016, http://spaceflight101.com/cz-5-maiden-flight/shijian-17-rendezvous-with-chinasat-5a/.
[32] Analytical Graphics (@AGItweets), "ComSpOC has detected that #Chinasat 5A has departed SJ-17 & is drifting 0.9 deg/day westward. SJ-17 remains @ 163 deg," Tweet, December 29, 2016, https://twitter.com/AGItweets/status/814513003798364161.
[33] Thomas M. Davis and David Melanson, "Xss-10 Micro-Satellite Flight Demonstration," Smartech.GATech.edu, accessed March 23, 2018, https://smartech.gatech.edu/bitstream/handle/1853/8036/SSEC_SD3_doc.pdf;jsessionid=906BB52FE69F848048883B704DB20F07.smart2.
[34] Lt Col Fred Kennedy, "Orbital Express Space Operations Architecture," DARPA Tactical Technology Office, accessed March 23, 2018, http://archive.darpa.mil/orbitalexpress/index.html.
[35] "Prisma," OHB Sweden, accessed March 23, 2018, http://www.ohb-sweden.se/space-missions/prisma/.
[36] Craig Covault, "Secret inspection satellites boost space intelligence ops," *Spaceflight Now*, January 14, 2009, http://www.spaceflightnow.com/news/n0901/14dsp23/.
[37] Mike Gruss, "Air Force sent GSSAP satellite to check on stalled MUOS-5," *SpaceNews,* August 18, 2016, http://spacenews.com/air-force-sent-gssap-satellite-to-check-on-stalled-muos-5/.

Table 1-1 - Recent Chinese Rendezvous and Proximity Operations

Date(s)	System(s)	Orbital Parameters	Notes
June – Aug. 2010	SJ-O6F, SJ-12	570-600 km; 97.6°	SJ-12 maneuvered to rendezvous with SJ-06F. Satellites may have bumped into each other.
July 2013 – May 2016	SY-7, CX-3, SJ-15	Approx. 670 km; 98°	SY-7 released an additional object that is performed maneuvers with and had a telerobotic arm. CX-3 performed optical surveillance of other in-space objects. SJ-15 Demonstrated altitude and inclination changes to approach other satellites.
Nov. 2016 – Feb. 2018	SJ-17, YZ-2 upper stage	35,600 km; 0°	YZ-2 upper stage failed to burn to the graveyard orbit and stayed near GEO. SJ-17 demonstrated maneuverability around the GEO belt and circumnavigated Chinasat 5A.

Potential Military Utility

The most likely military utility of the capabilities demonstrated by the SJ-12, SJ-15, and SJ-17 satellites is for on-orbit space situational awareness (SSA) and close-up inspections. Their operational pattern was consistent with slow, methodical, and careful approaches to rendezvous with other space objects in similar orbits. The satellites the SJ-12 and SJ-15 approached were in relatively similar orbits, differing in altitude by a couple hundred kilometers and slightly in inclination. They did not make huge changes to rendezvous with satellites in significantly different orbits. This behavior is similar to several U.S. RPO missions to test and demonstrate satellite inspection and servicing capabilities such as the XSS-11 (See U.S. Co-Orbital ASAT, Section 3-2).

The SJ-17's approach to Chinasat 5A was not inconsistent with the way other active satellites in the GEO belt relocate to different orbital slots. It is also not unusual for satellites to be co-located within several tens of kilometers to share a GEO slot, although it is rare for them to approach within 1 km as the SJ-17 eventually did. Such a close approach in GEO could be used for very detailed imaging or inspection of another satellite or to intercept radiofrequency signals directed at another satellite from Earth. Likely examples of the latter are the activities of the U.S. PAN satellite (35815, 2009-047A) between 2009 and 2014 (See U.S. Co-Orbital ASAT, Section 3-2), and the Russian Luch/Olymp satellite (40258, 2014-058A) in 2015 (See

Russian Co-Orbital ASAT; Section 2-2).

While the known on-orbit activities of the SJ-12, SJ-15, and SJ-17 did not include explicit testing of offensive capabilities or aggressive maneuvers, it is possible that the technologies they tested could be used for offensive purposes in the future. One potential offensive use would be to get a radio-frequency jammer close to a satellite, thereby greatly amplifying its ability to interfere with the satellite's communications. While possible, to date there is no direct public evidence of such systems being tested on orbit, although there have been multiple research articles published in Chinese journals discussing and evaluating the concept.[38]

The onboard tracking and guidance systems used for rendezvous could be used to try and physically collide with another satellite to damage or destroy it. However, the approach would have to involve much higher relative velocities than what the Chinese RPO satellites have demonstrated to date, and potentially involving higher velocities and longer closing distances than what these satellites are capable of. Furthermore, the deliberate maneuvering to create a conjunction with the target satellite would be detectable with existing processes already in place to detect accidental close approaches. Warning time of such a close approach would likely be at least hours (for LEO) or days (for GEO), unless the attacking satellite was already in a very similar orbit.

[38] David Chen, "Testimony before the U.S.-China Economic and Security Review Commission," Hearing on 'China's Advanced Weapons' Panel on China's Directed Energy and Electromagnetic Weapons Programs, February 23, 2017, https://www.uscc.gov/sites/default/files/Chen_Testimony.pdf.

1.2 - Chinese Direct-Ascent ASAT

Assessment

China has at least one, and possibly as many as three, programs underway to develop DA-ASAT capabilities, either as dedicated counterspace systems or as midcourse missile defense systems that could provide counterspace capabilities. China has engaged in multiple, progressive tests of these capabilities since 2005, indicating a serious organizational effort. Chinese DA-ASAT capability against LEO targets is likely mature and may be operationally fielded on mobile launchers within the next few years. Chinese DA-ASAT capability against deep space targets (MEO and GEO) is likely still in the experimental or development phase, and there is not sufficient evidence to conclude whether it will become an operational capability in the near future.

Specifics

Program Background

The Chinese direct-ascent ASAT program has its roots in several programs that emerged from the 1960s through the 1990s. Program 640, initially tasked with development of anti-ballistic missiles and surface-to-air missile (SAM) sites, began a dedicated ASAT program in 1970, and oversaw most of China's counterspace funding and development for the first two decades. During this period, nearly all Chinese ASAT work appears to have taken place within the various subsidiaries of the Fifth Academy of the Chinese Ministry of Defense, especially the No. 2 General Design Department of the Second Academy.[39]

These various subsidiaries have, over time, been consolidated into large state-owned companies, yet have retained deep-seated direct ties to the military—particularly with regard to development and use of ASAT technologies. Today, the General Design Department is a subsidiary of the China Aerospace Industry Corporation (CASIC), which is responsible, among other things, for a variety of derivatives of China's Dong-Feng ballistic missile series, including several with ASAT relevance.[40]

The emergence of this structure is important for understanding the character of China's counterspace development. First, there is often little division between the 'private' and 'public' sectors, or between civilian and military space. Second, it is likely that bureaucratic imperatives for rent-seeking and sustainment, coupled with institutional inertia and silos of information and decision-making authority, are giving elements of Chinese counterspace development a life of their own, much as they did in the United States and USSR during the Cold War. The number and

[39] Gregory Kulacki, "Anti-Satellite (ASAT) Technology in Chinese Open-Source Publications," Union of Concerned Scientists, July 1, 2009, http://www.ucsusa.org/sites/default/files/legacy/assets/documents/nwgs/Kulacki-Chinese-ASAT-Literature-6-10-09.pdf.
[40] Ibid.

diversity of counterspace programs may be driven by competition between organizations more than a deliberate strategy to have multiple competing programs.

Program 640 was shuttered in 1980. A few years later, Program 863—a broad umbrella program for cutting edge technological developments—took its place. In 1995, a kinetic kill vehicle (KKV) project began which was housed within Program 863.[41] Initial testing began in the late 1990s, followed by further vector and velocity control testing in 2003, at which point the system entered service as the interceptor for the HQ-19 missile defense system.[42] The HQ-19 is a solid-propelled high altitude hit-to-kill (HTK) intercept system roughly equivalent to the U.S. Terminal High Altitude Area Defense (THAAD) missile defense system. Since then, China has demonstrated significant advances in HTK capability, and engaged in large-scale modernization and development efforts for advanced rocket technology; tracking, targeting, and SSA capabilities; and launch infrastructure, both mobile and stationary.

Capabilities

China may be developing as many as three direct-ascent ASAT systems, although it is unclear whether all three are intended to be operational or whether their primary mission is counterspace or midcourse missile defense. The first known system is known as the SC-19, sometimes referred to as DN-1, and has been tested multiple times, as summarized in Table 1-2. The first known tests were in 2005 and 2006, both from Xichang Satellite Launch Center in Sichuan (See Xichang; Section 8-6), and appear to have been tests of the missile itself.[43] On January 11, 2007, the SC-19 was tested for the third time from Xichang and destroyed an aging Chinese FengYun 1C weather satellite at an altitude of 865 km, which created several thousand pieces of orbital debris.[44] The system was reportedly tested again in 2010 and 2013 from the Korla Missile Test Complex (See Korla West; Section 8-2) with successful intercepts of a ballistic target. The move from Xichang to Korla may indicate the system has entered a new phase of development, or possibly even operational testing.

[41] Mark Stokes and Dean Cheng, "China's Evolving Space Capabilities: Implications for U.S. Interests," report prepared for The US-China Economic and Security Review Commission, April 26, 2012, https://www.hsdl.org/?view&did=708400

[42] Ibid; Michael Pillsbury, "An Assessment of China's Anti-Satellite and Space Warfare Programs, Policies and Doctrines," report prepared for The US-China Economic and Security Review Commission, January 19, 2007, https://www.uscc.gov/sites/default/files/Research/An%20Assessment%20of%20China%27s%20Anti-Satellite%20And%20Space%20Warfare%20Programs.pdf; John Pike, "HQ-19 Anti-Ballistic Missile Interceptor," *GlobalSecurity.org*, last updated February 6, 2018, https://www.globalsecurity.org/space/world/china/hq-19.htm.

[43] Michael R. Gordon and David S. Cloud, "U.S. Knew of China's Missile Test, but Kept Silent," *The New York Times*, April 23, 2007, http://www.nytimes.com/2007/04/23/washington/23satellite.html.

[44] T.S. Kelso, "Analysis of the 2007 Chinese ASAT Test and the Impact of its Debris on the Space Environment," AMOS Conference Technical Papers, (2007): pp. 321-330. http://celestrak.com/publications/AMOS/2007/AMOS-2007.pdf.

Naming Convention for Chinese DA-ASATs

The naming conventions for Chinese DA-ASATs is complicated and uncertain. The U.S. intelligence community traditionally christens foreign missiles according to the launch site at which they were first observed, followed by a number indicating how many other unique missile types already bear that moniker. For example, SC-19 corresponds to the nineteenth missile type observed from Shuang cheng zi, the U.S. intelligence designation for Jiuquan Space Launch Center. The Chinese DA-ASATs have also been referred to as "DN", indicating shorthand for Dong Neng (动能), a Chinese phrase literally translating to "Kinetic Energy." Although this is somewhat in line with the taxonomy for China's own designations for its ballistic and cruise missiles, the Dong-Feng-XX (東風, literally "East Wind"), the only public mentions of the DN label have been in U.S. news reports citing anonymous U.S. officials. Thus, the DN-X designation may be a leak of the Chinese internal name for the system as divined by U.S. intelligence, or it could be an unofficial label created by outside sources.

While the specifications of the SC-19 are not publicly available, analysis of its technological foundations and demonstrated capabilities is revealing. The SC-19 appears to be based on the DF-21C ballistic missile, but also derives some elements from the HQ-19 missile defense system, including the intercept vehicle and certain rocket stages.[45] The DF-21 has an operational range of 2150-2500 km, which typically would amount to a vertical reach of about half that or approximately 1250 km. Subsequent analyses have concluded that while the SC-19 incorporates many design aspects of the DF-21, it may feature three solid stages and a liquid upper stage.[46]

The organizational history of the SC-19 yields further clues. Chinese rocket development is centralized in two state-owned corporations. According to Chinese bloggers, CASIC sought to leverage the DF-21 and its expertise in solid rockets to develop a new line of solid rocket space launch vehicles (SLV).[47] The first attempt was the Kaituozhe 1 (KT-1), a four-stage rocket 13.6 m in length and 1.4 m in diameter that was designed to place a 50 kg payload in a 400 km sun-synchronous orbit. Both known tests of the KT-1 failed, and the project was apparently canceled. A larger 1.7-meter diameter version called the KT-2 was planned but never developed. However, in 2002, CASIC won a contract to build a 1.4 m diameter, four-stage rocket (three solid stages with a liquid upper stage) called the KT-409 that was launched from a WS2500 TEL. This is likely the SC-19.

[45] Rick Fisher finds that the DF-21 forms the basis for the SC-19. See: Fisher, China's Military Modernization: Building for Regional and Global Reach, pp. 2, 131; MissileThreat provides an operational range of 2500 km for the DF-21, while think tank analyst Sean O'Connor pegs the range at 2150 km. See: "All Missiles," MissileThreat, George C. Marshall Institute and Claremont Institute, http://missilethreat.com/all-missiles/; Sean O'Connor, "PLA Ballistic Missiles," (Report prepared under contract APA-TR-2010-0802 for Air Power Australia in 2010, Last updated: 27 January 2014), http://www.ausairpower.net/APA-PLA-Ballistic-Missiles.html#mozTocId8319.

[46] Phillip C. Saunders and Charles D. Lutes, "China's ASAT Test: Motivations and Implications," *Joint Force Quarterly*, Issue 46, (2007): pp. 39-45, http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA517485.

[47] Brian Weeden, "Through a glass, darkly: Chinese, American, and Russian anti-satellite testing in space," *The Space Review*, March 17, 2014, http://www.thespacereview.com/article/2473/1.

Figure 3 - DF-21 MRBM
Missile version upon which the SC-19 is likely based, mounted atop a TEL.
Image credit: Defence Blog.[48]

China has also conducted at least one test of what is likely a DA-ASAT that might be able to reach higher orbits. On May 13, 2013, China launched a rocket from the Xichang Satellite Launch Center (See Xichang; Section 8-6), which the Chinese Academy of Sciences stated was a high-altitude scientific research mission.[49] A U.S. military official stated that "the launch appeared to be on a ballistic trajectory nearly to [GEO]. We tracked several objects during the flight…and no objects associated with this launch remain in space,"[50] but unofficial U.S. government sources say it was actually a test of a new ballistic missile related to China's ASAT program.[51] Subsequent launch analysis strongly supports this conclusion.

The details of the launch were different from those of either a standard satellite launch to GEO or the launch of a sounding rocket. The Notice to Airmen (NOTAM) released by China to provide advance warning of the flight path in case of complications covered a ground track lining up with

[48] Dylan Malyasov, "China displays DF-21D Anti-Ship Ballistic Missile," *Defence-Blog*, September 3, 2015, http://defence-blog.com/news/china-displays-df-21d-anti-ship-ballistic-missile.html.

[49] "中国再次高空科学探测试验: 高度更高数据更多," China News, May 14, 2013, http://www.chinanews.com/gn/2013/05-14/4817925.shtml.

[50] Marc V. Schanz, "Chinese Anti-Satellite Test?," *Air Force Magazine*, May 16, 2013, http://www.airforcemag.com/DRArchive/Pages/2013/May%202013/May%2016%202013/Chinese-Anti-Satellite-Test.aspx.

[51] Bill Gertz, "China Conducts Test of New Anti-Satellite Missile," *The Washington Free Beacon*, May 14, 2013, http://freebeacon.com/national-security/china-conducts-test-of-new-anti-satellite-missile/.

a GEO launch trajectory,[52] but stretching further south than either GEO satellite launches or a typical sounding rocket. The resultant rocket launch went far higher than a typical sounding rocket, and the rocket plume was much larger and more intense than would be expected with a sounding rocket. Moreover, there's no evidence that it "released a barium cloud" as claimed by CAS, nor has there been any subsequent scientific research published as a result of the launch.

Analysis of the launch site also points to something other than either an orbital or sounding rocket.[53] Both are typically larger and more complicated than ballistic missiles. As a result, they are usually launched from fixed launch pads, with standing support structures. In Xichang, however, there are only two official launch pads: one was unavailable at the time of the May 13 launch (as it was being retrofitted after use for the LM-3A), while the other played host to a LM-3B/E launch on May 1, leaving insufficient time to prep another SLV for launch.

Furthermore, the launch appeared to go much higher than the altitude claimed by the Chinese government. In their statement, CAS claimed the rocket reached 10,000 km[54], whereas the U.S. military claimed it went "nearly to GEO" at 36,000 km. U.S. officials also stated that the upper stages re-entered the Earth's atmosphere "over the Indian Ocean".[55] A technical analysis concluded that re-entry location is only possible if the apogee was at least 30,000 km; if the apogee was only 10,000 km, the Earth would not have had enough time to rotate for it to land in the Indian Ocean.[56] The flight trajectory is also far beyond what the SC-19 is believed to be capable of.

The most plausible explanation for the May 2013 launch was that it was a test of the rocket component of a new direct ascent ASAT weapons system derived from a road-mobile ballistic missile. Commercial satellite imagery shows a transporter-erector-launcher (TEL), most commonly associated with mobile ballistic missiles, located on a purpose-built launch pad towards the southeast corner of Xichang, as shown in Figure 4 below.[57] The pad is similar to the one believed to have been constructed for the SC-19 testing in the northwest of Xichang. A report from the U.S.-China Economic and Security Review Commission labeled this new rocket as DN-2 and claimed it may reach operational status in 2020-2025.[58] However, the only known sources of this

[52] "Chinese Officials provide initial Information on Monday's Sub-Orbital Launch," *Spaceflight101*, May 15, 2013, http://www.spaceflight101.net/chinese-rocket-launch-may-2013.html.
[53] Brian Weeden, "Through a glass, darkly: Chinese, American, and Russian anti-satellite testing in space," *The Space Review*, March 17, 2014, http://www.thespacereview.com/article/2473/1.
[54] Note that in the Chinese language, 10,000 is a base amount of something, so this may have been used as an order of magnitude statement rather than meant as an absolute distance. Still, it was less than forthcoming about the actual apogee of the test.
[55] Andrea Shalal-Esa, "U.S. sees China launch as test of anti-satellite muscle: source," *Reuters*, May 15, 2013, http://www.reuters.com/article/2013/05/15/us-china-launch-idUSBRE94E07D20130515.
[56] Brian Weeden, "Through a glass, darkly: Chinese, American, and Russian anti-satellite testing in space," *The Space Review*, March 17, 2014, http://www.thespacereview.com/article/2473/1.
[57] Ibid.
[58] "USCC 2015 Annual Report," pp. 294-294, November 2015, accessed March 23, 2018, https://www.uscc.gov/sites/default/files/annual_reports/2015%20Annual%20Report%20to%20Congress.PDF.

designation are news reports that cite anonymous U.S. defense officials,[59] so the veracity of the label is in question.

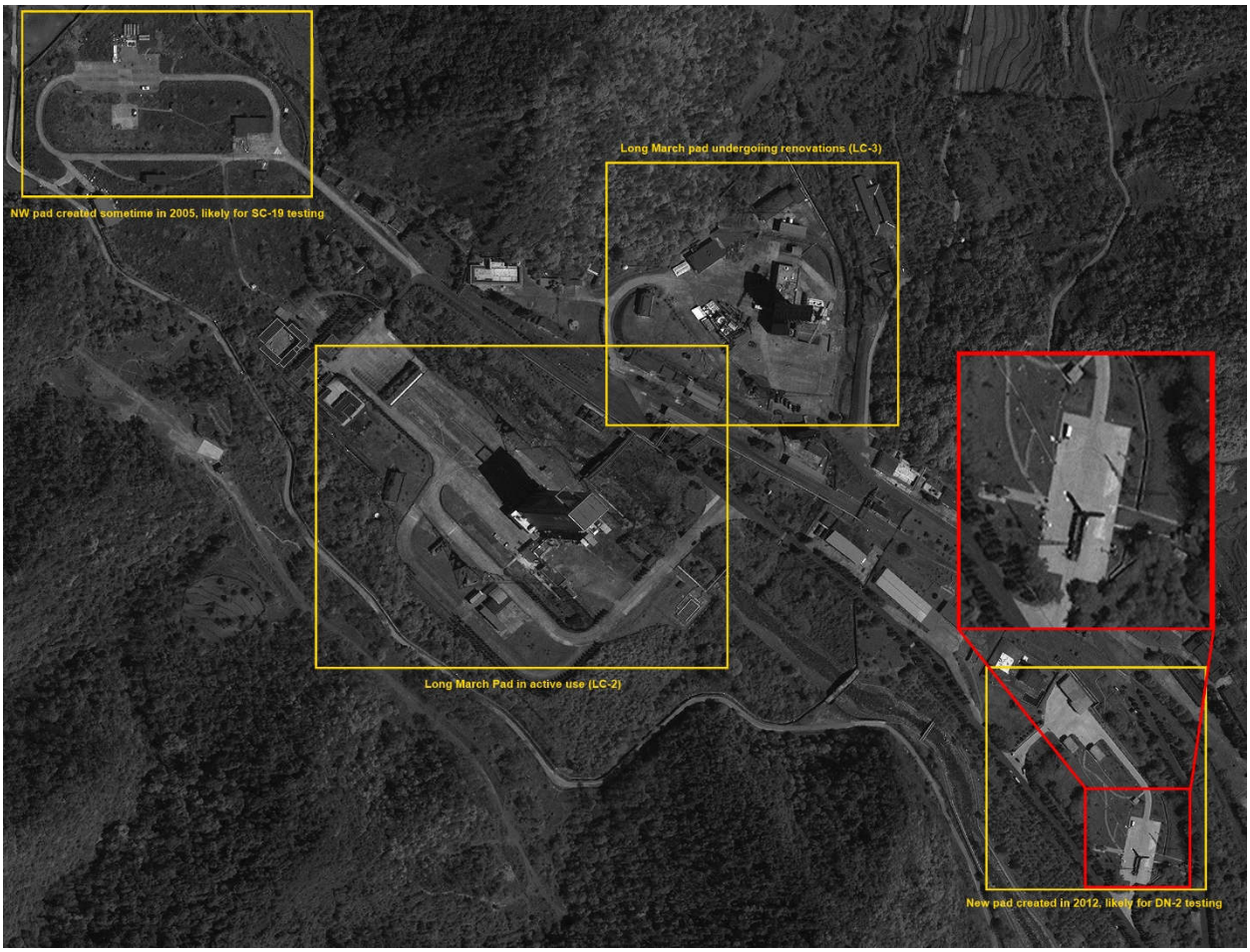

Figure 4 - Xichang from April 3, 2013
Imagery shows a TEL on the southeast pad.

In 2014, China conducted another rocket test, this time claiming that it was part of a missile defense interceptor program.[60] Very little information is available in the public record about this launch, other than that it occurred, remained suborbital, and does not appear to have had a clearly evident target, ballistic or otherwise. However, the United States government openly declared it an anti-satellite test—the only time since 2007 that any event has been so-labeled publicly. Asked for comment, then-Assistant Secretary of State for Arms Control, Verification, and Compliance Frank Rose noted on the record that "Despite China's claims that this was not an ASAT test, let me assure

[59] Bill Gertz, "China Conducts Test of New Anti-Satellite Missile," *The Washington Free Beacon*, May 14, 2013, http://freebeacon.com/national-security/china-conducts-test-of-new-anti-satellite-missile/.
[60] Mike Gruss, "U.S. State Department: China Tested Anti-satellite Weapon," *SpaceNews,* July 28, 2014, http://spacenews.com/41413us-state-department-china-tested-anti-satellite-weapon/.

you the United States has high confidence in its assessment, that the event was indeed an ASAT test."[61] A report published by the US-China Economic and Security Review Commission also stated that the 2014 test was of the SC-19/DN-1, but did not provide independent evidence.[62]

Since 2014, evidence suggests China has conducted at least three more tests that may be linked to their DA-ASAT program. A launch on October 30, 2015, from Korla created unusual contrails that were seen on Chinese social media.[63] Photos from another test on July 22, this time launched from Jiuquan Satellite Launch Center, were captured by a pilot on a Dutch commercial airliner flying over the Himalayas.[64] On February 5, 2018, Chinese state media announced it had carried out "land-based mid-course missile interception test within its territory."[65] In all three cases, anonymous U.S. officials were cited by news sources claiming that the tests were of a system known publicly as DN-3 and labeled by U.S. intelligence agencies as KO-09 (as the ninth missile type seen out of Korla).[66] However, there is no publicly-available evidence to support the claims that this was either an ASAT test, or that the DN-3 series is a dedicated ASAT weapon system. There is evidence to suggest that the DN series is actually a mid-course missile defense system, akin to the U.S. SM-3, with latent ASAT capabilities.[67]

[61] Mike Gruss, "Senior U.S. Official Insists China Tested ASAT Weapon," *SpaceNews*, August 25, 2014, http://spacenews.com/41676senior-us-official-insists-china-tested-asat-weapon/.
[62] "USCC 2015 Annual Report," pg. 293, November 2015, accessed March 23, 2018, https://www.uscc.gov/sites/default/files/annual_reports/2015%20Annual%20Report%20to%20Congress.PDF.
[63] Jing Heng, "网友11月1日拍到新疆库尔勒神奇天象 疑似航天或反导试验," *Guancha.cn*, November 1, 2015, http://www.guancha.cn/military-affairs/2015_11_01_339656.shtml.
[64] Tom Demerly, "Commercial Pilot Catches Remarkable Photos of Alleged Secret Chinese Anti-Missile Test," *The Aviationist*, July 29, 2017, https://theaviationist.com/2017/07/29/commercial-pilot-catches-remarkable-photos-of-alleged-secret-chinese-anti-missile-test/.
[65] Ankit Panda, "Revealed: The Details of China's Latest Hit-To-Kill Interceptor Test," *The Diplomat*, February 21, 2018, https://thediplomat.com/2018/02/revealed-the-details-of-chinas-latest-hit-to-kill-interceptor-test/.
[66] Bill Gertz, "China Carries Out Flight Test of Anti-Satellite Missile," *The Washington Free Beacon*, August 2, 2017, http://freebeacon.com/national-security/china-carries-flight-test-anti-satellite-missile/.
[67] Ankit Panda, "Revealed: The Details of China's Latest Hit-To-Kill Interceptor Test," *The Diplomat*, February 21, 2018, https://thediplomat.com/2018/02/revealed-the-details-of-chinas-latest-hit-to-kill-interceptor-test/.

Table 1-2 - History of Chinese DA-ASAT Tests [68]

Date	ASAT System	Site	Target	Apogee	Notes
July 7, 2005	SC-19	Xichang	None known	??	Likely rocket test
Feb. 6, 2006	SC-19	Xichang	Unknown satellite	??	Likely near-miss of orbital target
Jan. 11, 2007	SC-19	Xichang	FY-1C satellite	865 km	Destruction of orbital target
Jan. 11, 2010	SC-19	Korla	CSS-X-11 ballistic missile launched from Jiuquan	250 km	Destruction of target
Jan. 20, 2013	Possibly SC-19	Korla	Unknown ballistic missile launched from Jiuquan	Suborbital	Destruction of target
May 13, 2013	Possibly DN-2	Xichang	None known	~30,000 km	Likely rocket test
July 23, 2014	Possibly DN-2, (possibly SC-19)	Korla? (Jiuquan?)	Likely ballistic missile launched from Jiuquan	Suborbital	Likely intercept test
Oct. 30, 2015	Possibly DN-3	Korla	None known, possible ballistic missile	Suborbital	Likely rocket test
July 23, 2017	DN-3	Jiuquan?	Likely ballistic missile	Suborbital, malfunctioned	Likely intercept test
Feb. 5, 2018	DN-3	Korla	CSS-5 ballistic missile	Suborbital	Likely intercept test

There has been speculation by Western analysts that China may also have sea- or air-based capabilities that could be used as DA-ASATs. Some have suggested that the JL-2 submarine-launched ballistic missile (SLBM) developed for basing on China's JIN-class SSBNs may have an ASAT capability. Others have suggested China may be developing an air-launched DA-ASAT, similar to the U.S. ASM-135 (See U.S. Direct-Ascent ASAT; Section 3-8) or Russian Kontakt (See Russian Direct-Ascent ASAT; Section 2-12) systems. However, there is very little to no publicly-available evidence to support these claims, other than the theoretical possibility.

Potential Military Utility

China's 2007 ASAT test, and the subsequent ballistic intercepts, have demonstrated the ability to hit and destroy space objects using a KKV. Their heritage from road-mobile ballistic missiles indicates the systems may be mobile, which would create additional challenges for locating the threat prior to launch. However, the known tests to date have all occurred from prepared pads, leaving the possibility that a minimum level of infrastructure may be required.

[68] Data compiled from multiple sources.

Given the known testing, it is likely that China either has fielded, or could field, an operational DA-ASAT capability against most LEO satellites. This would include satellites performing military weather and ISR functions. China would have to wait for such satellites to overfly an area where one of the systems is deployed, but most LEO satellites would do so daily to every few days. However, once launched, the target would only have an estimated 5-15 minutes warning time before impact.

It is unlikely that China currently possesses an operational DA-ASAT capability against high altitude satellites in MEO or GEO orbits. Only one test, in May 2013, is known to have targeted higher altitudes, and given the unique nature of such a system, it would likely require multiple tests to become militarily useful. In addition, the primary target in MEO for such a system, the American military's Global Positioning System (GPS) navigation constellation, consists of more than 30 satellites distributed across multiple orbital planes. Many of the GPS satellites would need to be destroyed to have an appreciable impact on the GPS system, and their higher altitude (20,000 km) would provide at least an hour of warning time after launch. Other potential targets in the GEO belt, such as U.S. missile early warning, data relay, or electronic intelligence satellites, are much fewer in number and less distributed, making the capabilities easier to eliminate. However, their even higher altitude (36,000 km) would mean an even longer warning times of several hours after launch. The ability of the DA-ASAT kill vehicle to adjust for any changes in the target's trajectory over that time is unknown, and unlikely at present.

At the same time, there are also constraints on the military utility of such systems, particularly as China improves its own space capabilities. The use of a kinetic-kill DA-ASAT against an orbital target will invariably create large amounts of orbital space debris, as was seen in the 2007 test. Aggressive use of such a capability would invariably lead to widespread condemnation, as happened after the 2007 test and appears to have shaped Chinese testing practices since. Moreover, as China invests in and deploys its own military satellites and space capabilities, the long-lasting debris from the use of DA-ASATs will be increasingly likely to threaten their own capabilities. Use of a DA-ASAT would also be relatively easy to attribute to China. Thus, the military utility of DA-ASATs would have to be weighed against the potential costs, particularly relative to less destructive capabilities such as jamming or blinding.

1.3 - Chinese Policy and Doctrine

Chinese Views on Space Warfare

Official Chinese public statements on space warfare and space weapons have remained consistent: "China always adheres to the principle of the use of outer space for peaceful purposes and opposes the weaponization of or an arms race in outer space."[69] However, since 2015, other official writings suggest China's position on space warfare and space weapons has become more nuanced. China's 2015 defense white paper, China's Military Strategy, for the first-time designated outer space as a military domain and linked developments in the international security situation to defending China's interests in space. The defense white paper states that "Outer space has become a commanding height in international strategic competition. Countries concerned are developing their space forces and instruments, and the first signs of weaponization of outer space have appeared." As a result, "China will keep abreast of the dynamics of outer space, deal with security threats and challenges in that domain, and secure its space assets to serve its national economic and social development, and maintain outer space security."[70] In particular, the white paper states that "threats from such new security domains as outer space and cyberspace will be dealt with to maintain the common security of the world community." In 2015, defense of China's interests in space was made legally binding in China's National Security Law.[71]

Chinese Counterspace Doctrine

The Chinese military does not appear to have an official doctrine governing the use space in military operations and most of what can be assessed about Chinese thinking on the role of counterspace weapons must be based on unofficial Chinese military writings. This may change in the coming years, however. On December 31, 2015, the Chinese military established the Strategic Support Force, an organization intended, in part, to help unify the command and control of China's space forces and to make them more operationally responsive.[72] More recently, U.S. intelligence officials state that the PLA has "formed military units and begun initial operational training with counterspace capabilities that it has been developing, such as ground-launched ASAT missiles" toward the end of better integrating counterspace capabilities with other domains.[73]

---

[69] Statement by Ms. Pan Kun of the Chinese Delegation at the 71st Session of the UN General Assembly on Agenda Item 48: International Cooperation in the Peaceful Uses of Outer Space, October 13, 2016, http://www.china-un.org/eng/hyyfy/t1405942.htm.

[70] *China's Military Strategy*, White Paper issued by the State Council Information Office of the People's Republic of China, May 2015, accessed March 23, 2018, http://eng.mod.gov.cn/Database/WhitePapers/.

[71] "Authorized Release: National Security Law of the People's Republic of China," (授权发布：中华人民共和国国家安全法), *Xinhua*, July 1, 2015, http://news.xinhuanet.com/politics/2015-07/01/c_1115787801_3.htm.

[72] See Kevin L. Pollpeter, Michael S. Chase, and Eric Heginbotham, *The Creation of the Strategic Support Force and Its Implications for Chinese Military Space Operations*, (Santa Monica: RAND, 2017).

[73] Daniel Coats, "Worldwide Threat Assessment of the U.S. Intelligence Community," unclassified statement for the record before the Senate Armed Services Committee, March 6, 2018, https://www.dni.gov/files/documents/Newsroom/Testimonies/Final-2018-ATA---Unclassified---SASC.pdf

Nevertheless, Chinese thinking on space has remained consistent for at least the past two decades. According to the 2015 defense white paper, the PLA will "endeavor to seize the strategic initiative in military struggle" and "proactively plan for military struggle in all directions and domains."

Chinese analysts argue that China must develop counterspace weapons to balance U.S. military superiority and protect China's own interests.[74] As one researcher writes, China's development of ASAT weapons is to protect its own national security and adds that "only by preparing for war can you avoid war."[75] The authors of the 2013 Science of Military Strategy write that given the wide-range of rapid strike methods, "especially space and cyber attack and defense methods," China must prepare for an enemy to attack from all domains, including space.[76]

Chinese analysts assess that the U.S. military relies upon space for 70–90 percent of its intelligence[77] and 80 percent of its communications.[78] Based on this assessment, Chinese analysts surmise that the loss of critical sensor and communication capabilities could imperil the U.S. military's ability to achieve victory. In this context, the Chinese military seeks to deny the U.S. military use of information from its space-based assets. Chinese military analysts have noted the dependence of the U.S. military on space and have concluded that the loss of the use of space for the U.S. military may cause it to lose the conflict.

In addition to actual warfighting, space power can also be used to coerce. Chinese analysts write that having the ability to destroy or disable an opponent's satellites may deter an adversary from conducting counterspace operations against Chinese satellites. Space power can also improve the overall capabilities of a military and serve as a deterrent force not just against the use of specific types of weapons, but also as a general capability that can deter a country from even becoming involved in a conflict.[79]

Chinese military writings state that the goal of space warfare and space operations is to achieve space superiority. Space superiority is defined as "ensuring one's ability to fully use space while at the same time limiting, weakening, and destroying an adversary's space forces." It not only

---

[74] Xu Nengwu and Huang Changyun, "Space Deterrence: Changes in the U.S. Strategic Deterrence System and Global Strategic Stability" (**太空威慑**: **美国**战略威慑体系调整与全球战略稳定性), *Foreign Affairs Review* (**外交**评论), No. 5, 2014, p. 62; Xiao Lei, Qing Mu, and Wang Qu, "Who Stirs Up a Space War?" (谁在挑起太空战争？), *Decision & Information* (**决策与信息**), Vol. 2, No. 339, 2013, p. 18; Yang Caixia and Ai Dun, "On the Legality of the Development of ASATs for China" (论中国发展反卫星武器的合法性), *Journal of Journal of Beijing University of Aeronautics and Astronautics (Social Sciences Edition)* (**北京航空航天大学学**报（社会科学版）), Vol. 23, No. 2, March 2010, pp. 46, 47, 50.

[75] Jiang Yu, "Space Thunder: Development of Hard-Kill Antimissile Weapon and China's Antimissile Testing" (**太空惊雷 反**导硬杀伤武器的发展及中国反导试验), *Shipborne Weapons* (舰载武器), No. 2, 2010, p. 14.

[76] AMS, *Science of Military Strategy*, p. 102.

[77] Jiang and Wang, *Study of Space Operations*, p. 150.

[78] Chang Xianqi, Military Astronautics (军事航天学), (Beijing: National Defense Industry Press, 2002), 257–58.

[79] Jiang Lianju and Wang Liwen (Eds.), *Textbook for the Study of Space Operations* (**空**间作战学教程), Beijing: Military Science Publishing House, 2013, 127.

includes offensive and defensive operations in space against an adversary's space forces, but also air, ground, and naval operations against space assets.

Chinese writers make the oft-repeated statement that "whoever controls space will control the Earth" and that outer space is the new high ground of military operations. They assert that the center of gravity in military operations has transitioned from the sea to the air and is now transitioning to space.[80] According to a textbook published by the Chinese military's top think tank, the Academy of Military Sciences (AMS), "Whoever is the strongman of military space will be the ruler of the battlefield; whoever has the advantage of space has the power of the initiative; having 'space' support enables victory, lacking "space" ensures defeat."[81] The authors of the influential Science of Military Strategy, also published by AMS, similarly conclude that space is the new high ground and that without space superiority one is at a disadvantage in all other domains.[82]

Chinese military writings overall place a heavy emphasis on gaining the initiative at the outset of a conflict, including during the deployment stage. Looking at the 1991 Gulf War, and the initial invasions of Afghanistan in 2001 and Iraq in 2003, Chinese military analysts assess that the PLA cannot allow the U.S. military to become fully prepared lest they cede victory. According to the authors of Study of Space Operations, China will "do all it can at the strategic level to avoid firing the first shot,"[83] but recommend that China should "strive to attack first at the campaign and tactical levels in order to maintain the space battlefield initiative."[84] They also argue that fighting a quick war is one of the "special characteristics of space operations" and that a military should "conceal the concentration of its forces and make a decisive large-scale first strike."[85]

Chinese Counterspace Budget

Little reliable information has been provided on the budget for China's entire space program, let alone its budget for counterspace technologies. It is likely that in relative terms, China spends much less on space than the United States, yet still manages to fund an extensive and robust program. According to one 2012 source, China invests less than 0.1 percent of its GDP on its space program. If correct, this would have placed China's annual spending on its entire space program

---

[80] Jiang Lianju and Wang Liwen (Eds.), Textbook for the Study of Space Operations (空间作战学教程), Beijing: Military Science Publishing House, 2013, p. 14.

[81] Jiang Lianju and Wang Liwen (Eds.), *Textbook for the Study of Space Operations* (空间作战学教程), Beijing: Military Science Publishing House, 2013, p. 1.

[82] China Academy of Military Science (AMS) Military Strategy Studies Department, *Science of Military Strategy* (战略学), Beijing: Military Science Press, December 2013; p. 96.

[83] Jiang Lianju and Wang Liwen (Eds.), *Textbook for the Study of Space Operations* (空间作战学教程), Beijing: Military Science Publishing House, 2013, p. 42.

[84] Jiang Lianju and Wang Liwen (Eds.), *Textbook for the Study of Space Operations* (空间作战学教程), Beijing: Military Science Publishing House, 2013, p. 52.

[85] Jiang Lianju and Wang Liwen (Eds.), *Textbook for the Study of Space Operations* (空间作战学教程), Beijing: Military Science Publishing House, 2013, pp. 142-143.

below $8.227 billion.[86] However, any estimate of China's spending and budget should be seen with a great deal of skepticism.

[86] Feng Shuxing, Reflection on Development of Space Power and Space Security (**我国空**间力量发展与空间安全的思考), Journal of Academy of Equipment(**装**备学院学报), October 2012, p. 9.

2 – RUSSIAN FEDERATION

Over the last two decades, Russia has refocused its effort on regaining many of the space capabilities it lost following the end of the Cold War. For the first several decades of the Space Age, the Soviet Union developed a robust set of governmental space programs that matched, or exceeded, the United States in many areas. While often not quite a technologically advanced as their American counterparts, the Soviets nonetheless managed to field significant national security space capabilities.

During the Cold War, the Soviet Union developed a range of counterspace capabilities as part of its strategic competition with the United States. Many of these capabilities were developed for specific military utility, such as destroying critical American military satellites, or to counter perceived threats, such as the Reagan Administration's Strategic Defense Initiative. Some of them underwent significant on-orbit testing and were considered operationally deployed. However, the Soviet Union also signed bilateral arms control agreements with the United States that put limits on the use of counterspace capabilities against certain satellites. Many of these programs were scrapped or mothballed in the early 1990s as the Cold War ended and funding dried up.

There is strong evidence that Russia has embarked on a set of programs over the last decade to regain some of its Cold War-era counterspace capability. In some cases, the evidence suggests legacy capabilities are being brought out of mothballs, and in other cases the evidence points to new, modern versions being developed. In all cases, Russia has a strong technical legacy to draw upon. Under Putin, Russia also has renewed political will to obtain counterspace capabilities for much the same reasons as China: to bolster its regional power and limit the ability of the United States to impede on Russia's freedom of action.

Unlike China, there is also significant evidence that Russia is actively employing counterspace capabilities in current military conflicts. There are multiple, credible reports of Russia using jamming and other electronic warfare measures in the conflict in eastern Ukraine, and indications that these capabilities are tightly integrated into their military operations.

The following sections summarize Russian counterspace development across co-orbital, direct ascent, directed energy, and electronic warfare categories, along with a summary of Russia's policy and doctrine on counterspace.

2.1 - Russian Co-Orbital ASAT

Assessment

During the Cold War, the Soviet Union engaged in a comprehensive program of development, testing, and operational deployment of a co-orbital ASAT capability with a demonstrated ability to intercept LEO satellites. Since 2010, Russia has been testing technologies for close approach and rendezvous in both LEO and GEO that could lead to a co-orbital ASAT capability, and some of those efforts have links to a Cold War-era LEO co-orbital ASAT program. However, the technologies could also be used for non-aggressive applications, and the on-orbit testing done to date does not conclusively prove they are for an ASAT program.

Specifics

During the Cold War, the Soviet Union had multiple efforts to develop, test, and deploy co-orbital ASAT capabilities. Many different concepts for deployment of co-orbital weapons were considered, including lasers, missile platforms, manned and unmanned gunnery platforms, robotic manipulators, particle beams, shotgun-style pellet cannons, and nuclear space mines, but most died on the drawing board. HTK co-orbital ASATs are one of the few known to have achieved operational status.

IS and IS-M

The first known serious effort was the Istrebitel Sputnikov (IS) or "satellite fighter" system, which was conceived in the late 1950s and began development in the 1960s.[87] The system featured a launch vehicle based on the R-36 (US designation SS-9) missile based from dedicated launch pads at Baikonur Cosmodrome in southern Kazakhstan. After being launched into orbit, the interceptor would separate from the booster, make multiple changes to its orbit so that it passed close to the target object, and then explode to release shrapnel that had an approximate effective range of 50 m. A shortcoming of the system is that it needed at least two orbits to do this, and the target object had several hours to detect the attack and alter its own trajectory.

The IS system was tested in orbit multiple times over three decades, with several actual intercepts against targets between 230 and 1,000 km and the creation of nearly 900 pieces of orbital space debris larger than 10 cm.

[87] Anatoly Zak, "IS Anti-satellite System," *Russian Space* Web, last modified July 13, 2017, http://www.russianspaceweb.com/is.htm.

Table **2-1** below shows the known tests of the IS system and its follow-ons. The first round of testing began in 1963 and concluded in 1971, after which the system was declared operational in February 1973.[88]

From 1976-77, eight additional tests of the system were conducted, publicly demonstrating an ability to operate effectively in a broader swathe of orbits from 150 to 1,600 km, culminating in the deployment of an upgraded version of the system, dubbed IS-M.[89] IS-M was allegedly capable of targeting satellites at altitudes of up to 2200 km, and inclinations of 50 to 130 degrees, with an estimated kill probability of 70-80 percent.[90] IS-M also reduced attack time by increasing speed and maneuverability to allow rendezvous with the target in a single orbit.[91] The final test of the IS-M system occurred in 1982; in 1983 a moratorium was declared on all ASAT tests, though modernization efforts apparently continued.

[88] Bart Hendrickx, "Naryad-V and the Soviet Anti-Satellite Fleet," *Space Chronicle*, Vol 69, 2016, available at http://www.bis-space.com/belgium/wp-content/uploads/2016/09/Naryad-V-and-the-Soviet-Anti-Satellite-Fleet.pdf.
[89] Ibid.
[90] Pavel Podvig, "Is China Repeating the Old Soviet and U.S. Mistakes?", *Russian Strategic Nuclear Forces*, January 19, 2007, http://russianforces.org/blog/2007/01/is_china_repeating_the_old_sov.shtml.
[91] Laura Grego, "Á History of Anti-Satellite Programs," *Union of Concerned Scientists*, January 2012, https://www.ucsusa.org/sites/default/files/legacy/assets/documents/nwgs/a-history-of-ASAT-programs_lo-res.pdf.

Table 2-1 - IS Tests Conducted by the Soviet Union[92]

Date of Test	Target Object	Interceptor	Notes
Nov. 1, 1963	None	Polyot 1	Engine and maneuvering test
Apr. 12, 1964	None	Polyot 2	Engine and maneuvering test
Oct. 27, 1967	None	Cosmos 185 (IS)	First test launch of IS interceptor
Oct. 20, 1968	Cosmos 248	Cosmos 249, Cosmos 252 (IS)	Attacked twice: by Cosmos 249 on Oct 20 and by Cosmos 252 on Nov 1
Oct. 23, 1970	Cosmos 373	Cosmos 374, Cosmos 375(IS)	Attacked twice: by Cosmos 374 on Oct 23 and by Cosmos 375 on Oct 30
Feb. 25, 1971	Cosmos 394	Cosmos 397 (IS)	
Mar. 18, 1971	Cosmos 400	Cosmos 404 (IS)	
Dec. 3, 1971	Cosmos 459	Cosmos 462 (IS)	
Feb. 16, 1976	Cosmos 803	Cosmos 804, Cosmos 814 (IS)	Attacked twice: by Cosmos 803 on Feb. 12 and by Cosmos 804 on Feb. 16
July 9, 1976	Cosmos 839	Cosmos 843 (IS)	
Dec. 17, 1976	Cosmos 880	Cosmos 886 (IS)	
May 23, 1977	Cosmos 909	Cosmos 910, Cosmos 918 (IS)	Attacked twice: by Cosmos 910 on May 23 and by Cosmos 918 on Jun 17 (both failures)
Oct. 26, 1977	Cosmos 959	Cosmos 961 (IS)	
Dec. 21, 1977	Cosmos 967	Cosmos 970 (IS)	Missed target, used as target itself in following test
May 19, 1978	Cosmos 970	Cosmos 1009 (IS)	
Apr. 18, 1980	Cosmos 1171	Cosmos 1174 (IS)	
Feb. 2, 1981	Cosmos 1241	Cosmos 1243, Cosmos 1258 (IS)	Attacked twice: Cosmos 1243 on Feb. 2 and Cosmos 1258 on Mar. 14 (both failures)
June 18, 1982	Cosmos 1375	Cosmos 1379 (IS-P)	

[92] Data compiled from multiple sources and available here: https://docs.google.com/spreadsheets/u/1/d/1e5GtZEzdo6xk41i2_ei3c8jRZDjvP4Xwz3BVsUHwi48/edit?usp=drive_web.

Soviet documents from the late 1980s indicate there were two more planned upgrades to the IS system, the IS-MU (14F10) and the IS-MD (75P6), also known as Naryad. IS-MU was designed to be an even more capable LEO co-orbital interceptor, and the IS-MD would be able to intercept satellites in GEO. There are no records of either system moving past the drawing board or confirmation of being tested in space, and both were ended in 1993. However, some components, including the network's SSA, targeting, and control systems, are known to have been maintained in working condition and also to have undergone comprehensive upgrades and modernization over the last decade.

Naryad

Towards the end of the Cold War, the Soviet Union began development of a new and more capable co-orbital system known as Naryad-V (14F11). The key technologies of the Naryad-V were a silo-based solid fuel rocket launch vehicle derived from the UR-100NUTTH (SS-19) paired with a new and very capable liquid fuel upper stage. The combination was designed to allow the system to target an extremely wide range of orbits between 0 to 130 degrees inclination and altitudes of 150 to 40,000 km,[93] and rapid launches of large numbers at once. At one meeting regarding the program in 1990, the prospect was discussed of launching as many as one hundred in a single volley.[94]

As with the later versions of the IS, the Naryad development was cut short by the fall of the Soviet Union. Table 2-2 below shows the known testing history of the Naryad program. The Naryad launch vehicle had two sub-orbital flight tests in November 1990 and December 1991, both from Baikonur Cosmodrome.[95] A third orbital flight test from Baikonur was conducted in December, with Rockot booster delivering the Radio ROSTO amateur radio satellite into a 1,900 by 2,145 km orbit.[96] It is rumored that the launch had a second payload, which may have been the Naryad interceptor, that fragmented shortly after launch. Eight pieces of orbital space debris were cataloged and are currently being tracked, along with the ROSTO satellite.

[93] Pavel Podvig, "Is China Repeating the Old Soviet and U.S. Mistakes?", *Russian Strategic Nuclear Forces*, January 19, 2007, http://russianforces.org/blog/2007/01/is_china_repeating_the_old_sov.shtml.
[94] Bart Hendrickx, "Naryad-V and the Soviet Anti-Satellite Fleet," *Space Chronicle*, Vol 69, 2016, available at http://www.bis-space.com/belgium/wp-content/uploads/2016/09/Naryad-V-and-the-Soviet-Anti-Satellite-Fleet.pdf" and Pavel Podvig, "Did Star Wars Help End the Cold War? Soviet Response to the SDI Program," *Russian Forces*, March 17, 2013, http://russianforces.org/podvig/2013/03/did_star_wars_help_end_the_col.shtml, p.18.
[95] Anatoly Zak, "UR-100", *Russian Space Web*, updated June 27, 2013, http://www.russianspaceweb.com/baikonur_ur100.html; "Rockot Launch Vehicles," updated December 24, 2017, http://www.russianspaceweb.com/rockot.html.
[96] Mark Wade, "Radio," *Astronautix*, Accessed March 22, 2018, http://www.astronautix.com/r/radio.html.

Table 2-2 - Suspected Naryad flight tests

Date	Booster	Payload	Launch Site	Launch Pad	Orbit
Nov. 20, 1990	Rockot/Briz-K	Naryad-V anti-satellite	Baikonur	Site 131	Sub-orbital
Dec. 20, 1991	Rockot/Briz-K	Experimental, Naryad test?	Baikonur	Site 175/1	Sub-orbital
Dec. 26, 1994	Rockot/Briz-K	Radio-ROSTO, Naryad test?	Baikonur	Site 175/1	1,900 km; 65°

After the fall of the Soviet Union, the components of the Naryad program found new commercial uses, leading to speculation that the program could be revived. The rocket has become the Rockot commercial launch vehicle operating from Plesetsk Cosmodrome, which has had 18 successful launches and placed more than 40 satellites into orbit.[97] The Naryad upper stage was developed into the Briz-KM and Briz-M, which are mainstays of Russian space launches to GEO.[98] Russian military officials have claimed that some "basic [ASAT] assets [were] retained" in connection to the "Naryad-VN" and "Naryad-VR" systems, to be employed if the United States or China were to put weapons in space.[99] It remains unclear precisely what those designations refer to, or what the difference between the two sub-systems might be.

Recent Rendezvous and Proximity Operations

More recently, a resurgence of Russian rendezvous and proximity operations (RPO) has driven substantial anxiety in the United States and elsewhere over concerns that they are aimed at developing new co-orbital ASAT capabilities. Since 2013, Russia has launched several satellites into LEO and GEO that have demonstrated the ability to rendezvous with other space objects, and in some cases do so after periods of dormancy.

The first known event was on December 25, 2013, when a Russian Rockot launch vehicle from Plesetsk Cosmodrome (See Plesetsk; Section 8-8) placed three small satellites into LEO in what appeared to be another routine launch to replenish the Rodnik constellation.[100] The Rodnik satellites are the current generation of store-and-dump communications satellites, which store messages uploaded from end users and then downlink them when the satellite passes over a receiving station. The launch was publicly announced, and shortly afterwards the Russian Defense Ministry announced that the three spacecraft had successfully separated from the upper stage. However, U.S. military cataloged a fourth payload from the launch, and over the following months,

[97] For an updated list of Rokot launches, see http://en.wikipedia.org/wiki/Rokot#Launch_table.
[98] Anatoly Zak, "Briz-K/KM," *Russian Space Web*, updated March 11, 2016, http://www.russianspaceweb.com/briz.html.
[99] Anatoly Zak, "Russian Anti-Satellite Systems," *Russian Space Web*, updated November 30, 2017, http://www.russianspaceweb.com/naryad.html; Anatoly Zak, "The Hidden History of Soviet Satellite-Killer," *Popular Mechanics*, November 1, 2013, https://www.popularmechanics.com/space/satellites/a9620/the-hidden-history-of-the-soviet-satellite-killer-16108970/.
[100] 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.

evidence emerged from official and open sources to confirm it.[101] Although Cosmos 2491 did not make any significant changes to its orbit, and there's credible evidence to suggest it has a civilian function, the secrecy of the launch and the Naryad legacy of the booster created concern among some analysts.

On May 23, 2014, another Rockot launch took place from Plesetsk with what appeared to be another Rodnik replenishment mission. Once again, the Russian government publicly declared that the launch carried three military satellites. Two days later, hobbyist satellite observers indicated that a fourth payload, Cosmos 2499, was on the launch. By mid-June, hobbyists reported that Cosmos 2499, had begun a series of maneuvers to match orbits with the Briz-KM upper stage that placed it in orbit.[102] The process took several months, and it was not until the end of November when Cosmos 2499 passed within a kilometer of the Briz-KM.[103] Amateur radio operators also reported that Cosmos 2499 appeared to be using the same radio frequencies as Cosmos 2491, suggesting they used the same Yubileiny-2 microsatellite bus.[104] After drifting apart, Cosmos 2499 did another series of maneuvers in January 2015 to put itself in an orbit that kept it a few kilometers above a several hundred kilometers away from the Briz-KM. On March 26, 2016, Cosmos 2499 made another orbit adjustment that slowly brought it closer to the Briz-KM by about tens of kilometers per day.

On March 31, 2015, a third Rockot launch took place from Plesetsk with what was publicly declared as carrying three Gonets-M satellites and a classified military payload. The Gonets serve as a civilian version of the Strela/Rodnik store-and-dump LEO communications constellation. The fourth payload, Cosmos 2504, began a small series of maneuvers in early April to bring it close to the Briz-KM upper stage that placed it in orbit. At some point during that pass, the Briz-KM's orbit was disturbed by an unknown perturbation, which could have been the result of a minor collision between the two space objects. If it was, the impact was very slight and did not result in additional debris being generated. It is also unknown if the impact was planned or was an accident. On July 3, 2015, Cosmos 2504 made another significant maneuver, lowering both its apogee and perigee significantly by around 50 km each, further separating itself from the Briz-M. On March 27, 2017, after more than a year of dormancy, Cosmos 2504 made a series of maneuvers that lowered its orbit, and on April 20, it passed within two km of a piece of Chinese space debris from their 2007 ASAT test.[105] This suggests that Cosmos 2504 has a satellite inspection or observation

[101] Jonathan McDowell, "Jonathan's Space Report No. 697," May 17, 2014, http://planet4589.org/space/jsr/back/news.697.
[102] Thread at the Novosti Kosmonavtiki forums, dated May 16, 2014, http://novosti-kosmonavtiki.ru/forum/forum12/topic14232/?PAGEN_1=5.
[103] Posting on the Novosti Kosmonavtiki forums, dated November 28, 2014, http://novosti-kosmonavtiki.ru/forum/messages/forum12/topic14778/message1315049/#message1315049.
[104] Пашков, Дмитрий, "Cosmos-2491/RS-46 (R4UAB)," *Youtube*, December 2, 2014, https://www.youtube.com/watch?v=jHKoSdhMVDk#t=14. The Russian government publicly disclosed the existence of the amateur radio payloads, which were activated at the end of the main mission.
[105] Anatoly Zak, "Russia Goes Ahead with Anti-Satellite System," *Russian Space Web*, updated December 15, 2017, http://www.russianspaceweb.com/Cosmos-2504.html.

mission and may have been looking for intelligence on the Chinese direct ascent interceptor program.

On June 23, 2017, a Russian Soyuz 2-1v rocket was launched from Plesetsk with two military payloads. One payload was rumored to be the first of the new series of military geodetic satellites, used to create extremely precise maps of the Earth's shape and gravitational field.[106] Russian officials declared that the launch also included a "space platform which can carry different variants of payloads" which was designated Cosmos 2519.[107] In late August, Cosmos 2519 made a series of small maneuvers. Publicly-available information strongly suggests that Cosmos 2519 has a remote sensing mission.[108] Shortly thereafter on August 23, Russian officials announced that a small satellite, designated Cosmos 2521, had separated from the platform and was "intended for the inspection of the condition of a Russian satellite."[109] Cosmos 2521 began making a series of small maneuvers in late August and early September, the purpose of which was unknown. It is speculated that Cosmos 2521 may be waiting for its orbit to align properly to rendezvous with Cosmos 2486, a Russian military optical surveillance satellite.[110] Subsequently, Russia reported that the satellite-inspector completed a series of proximity operations experiments and returned to the Cosmos 2519 host satellite on October 26.[111] On October 30, Russia announced that another small satellite, Cosmos 2523, separated from Cosmos 2521 and would have a satellite inspection function.[112] As of March 2018, Cosmos 2521 had not maneuvered to approach any other space objects.

Recent Russian RPO activities have also occurred in GEO. On September 28, 2014, a Proton-M SLV was launched from Baikonur Cosmodrome. Onboard was a satellite built for the Russian Ministry of Defence and Federal Security Service (FSB), which was destined for the GEO region. The name of the satellite is unknown, with manufacturer documents referring to it as "Olymp" or "Olymp-K" and public reference to it as "Luch," which is a series of Russian "bent pipe" data relay satellites.[113] The official Russian designation is Cosmos 2501.

The launch proceeded the same as many other Russian GEO launches. The initial set of burns placed the Briz-M upper stage and payload into an initial highly elliptical transfer orbit. Roughly

---

[106] Anatoly Zak, "Soyuz-2-1v Launches a Secret Satellite," *Russian Space Web*, August 30, 2017, http://www.russianspaceweb.com/napryazhenie.html.
[107] "Спутник 'Космос-2519' Минобороны РФ будет фотографировать космические объекты [Sputnik 'Cosmos-2519' of the Russian Defense Ministry Will Photograph Space Objects]," *MilitaryRussia.ru*, June 24, 2017, http://www.militarynews.ru/story.asp?rid=1&nid=454841.
[108] Bart Hendrickx, posting on the NASAspaceflight.com Forums, February 27, 2018, https://forum.nasaspaceflight.com/index.php?PHPSESSID=35dsgsej5k8tt51h7fo7re8e04&topic=43064.msg1793720#msg1793720.
[109] "С запущенного в интересах Минобороны космического аппарата выведен в космос спутник-инспектор," *Interfax.ru*, August 23, 2017, http://www.interfax.ru/russia/576068.
[110] "Russian Inspector Satellite set out on Orbital Endeavors with Fellow Kosmos Satellite," *Spaceflight101*, August 28, 2017, http://spaceflight101.com/russian-inspector-satellite-orbital-activity/.
[111] Jonathan McDowell, "Jonathan's Space Report No. 742," November 25, 2017, http://planet4589.org/space/jsr/back/news.742
[112] Bart Hendrickx, posting on the NASAspaceflight.com forums, March 3, 2018, https://forum.nasaspaceflight.com/index.php?topic=43064.msg1795369#msg1795369.
[113] Anatoly Zak, "Proton Successfully Returns to Flight Delivering a Secret Olymp Satellite," R*ussian Space Web* October 19, 2015, http://www.russianspaceweb.com/olymp.html.

nine hours after launch, the Briz-M upper stage executed a burn to (mostly) circularize the orbit at near GEO altitude and also zero out the inclination. After separating from Cosmos 2501, the Briz-M then conducted another burn to boost it out of the active GEO belt and into a disposal orbit above GEO in accordance with the IADC debris mitigation guidelines.

Over the next several months, Cosmos 2501 conducted a series of maneuvers that brought it close to other operational satellites around the GEO belt. The launch process left Cosmos 2501 at approximately 57 degrees east longitude, roughly due south of Yemen and the tip of the Arabian Peninsula. It originally began to drift eastward, towards the Indian Ocean, but around October 7, changed its orbit to begin drifting westward back towards Africa at a relatively high rate. Towards the end of October, it began to slow its drift rate, and around October 28, appeared to settle into position at around 52–53 degrees east. The only known Russian orbital slot nearby was that of the Express AM-6, a Russian commercial communications satellite that was launched on October 21, 2014. Cosmos 2501 stayed in this general area for nearly three months.

In late January 2015, Cosmos 2501 began to move again. By January 31, it had begun to drift eastwards again, at what began as a fairly high rate and slowed over time. It eventually arrived near 95–96 degrees east longitude, almost due south from Myanmar, around February 21. Observers once again wondered why Cosmos 2501 was in this area and hypothesized that it might be due to the presence of the Russian Luch 5V satellite, which was launched on April 28, 2014.

Around April 4, 2015, Cosmos 2501 began to move again. This time it began to drift westward at a lower rate, eventually coming to a stop around 18.1 degrees west, due south of the very western tip of Africa, on June 25, 2015. Observers began to wonder why it stopped at this location, noticing that there were no Russian satellites in the area. However, this location did place Cosmos 2501 right in between two operational Intelsat satellites, Intelsat 7 at 18.2 degrees west and Intelsat 901 at 18 degrees west, where it remained until mid-September.

On September 25, 2015, Cosmos 2501 left its parking spot between the Intelsat satellites and began to drift again, heading westward. Over the next several months, it made several more stops around the GEO belt, as documented in Table 2-3 below.

Table 2-3 - Longitudinal History of Cosmos 2501

Start Date	End Date	Longitude
Oct. 18, 2014	Dec. 28, 2014	54.0E
Jan. 2, 2015	Jan. 28, 2015	52.9E
Feb. 21, 2015	Apr. 4, 2015	96.0E
June 26, 2015	Sept. 25, 2015	18.1W
Oct. 5, 2015	Dec. 8, 2015	24.3W
Jan. 9, 2016	Aug. 30, 2016	1.1W
Sept. 14, 2017	July 27, 2017	9.9E
Aug. 17, 2017	-	32.7E

Table 2-4 - Recent Russian Rendezvous and Proximity Operations

Date(s)	System(s)	Orbital Parameters	Notes
June 2014 - March 2016	Cosmos 2499, Briz-KM R/B	1501 x 1480 km; 82.4°	Cosmos 2499 did series of maneuvers to bring it close to, and then away from, the Briz-KM upper stage.
April 2015 – April 2017	Cosmos 2504, Briz-KM R/B,	1507 x 1172 km; 82.5°	Cosmos 2504 maneuvers to approach the Briz-KM upper stage and may have had a slight impact before separating again.
March-April 2017	Cosmos 2504, FY-1C Debris	1507 x 848 km; 82.6°	After a year of dormancy, Cosmos 2504 did a close approach with a piece of Chinese space debris from the 2007 ASAT test
Oct. 2014 – Aug. 2017	Cosmos 2501, Express AM-6, Intelsat 7, Intelsat 901	35,600 km, 0°	Cosmos 2501 (Luch or Olym-K) parked near several satellites over nearly three years, including the Russian Express AM-6 and the American Intelsat 7 and Intelsat 401 satellites.
Aug – Oct 2017	Cosmos 2521, Cosmos 2486	670 x 650 km; 97.9°	Cosmos 2521 separated from Cosmos 2519 and performed a series of small maneuvers to do inspections before redocking with Cosmos 2519.

Potential Military Utility

The most likely military utility for the Cosmos 2499, Cosmos 2504, and Cosmos 2519 satellites is for on-orbit inspection and surveillance. Although the program appears to share some heritage with the Naryad program, their actual behavior on orbit has been different than that of the IS kinetic co-orbital interceptor. The operational pattern of the Cosmos 2499, Cosmos 2504, and Cosmos 2521 satellites is consistent with slow, methodical, and careful approaches to rendezvous with other space objects in similar orbits. The other space objects they approached were in largely similar orbits to their own, and only involved changes in altitude or phasing and not significant changes in inclination. This behavior is similar to several U.S. RPO missions to test and demonstrate satellite inspection and servicing capabilities, in particular XSS-11 and Orbital Express (See U.S. Co-Orbital ASAT; Section 3-2).

Cosmos 2501's approach to the other satellites in GEO was consistent with the way other active satellites in the GEO belt relocate to different orbital slots. It is also not unusual for satellites to be co-located within several tens of kilometers to share a GEO slot, although it is rare for them to approach within the 10 km that Cosmos 2501 eventually did. The evidence strongly suggests Cosmos 2501 is intended for a surveillance or intelligence mission. Documents from Russian industry indicate links to a military satellite communications program, and possible heritage to the Luch series of relay satellites. The on-orbit behavior of Cosmos 2501 indicates a potential mission to intercept broadcasts aimed at other GEO satellites, and possibly also to inspect other GEO satellites. Likely examples of the former are the activities of the U.S. PAN satellite (35815, 2009-047A) between 2009 and 2014, and the Chinese SJ-17 satellite (40258, 2014-058A) in 2017 (See Chinese Co-Orbital ASAT; Section 1-2). However, another plausible theory is that Cosmos 2501 is serving as a relay satellite for the Russian Navy, as its changes in orbit are somewhat linked to Russian Naval deployments in the Atlantic, Indian, and Pacific Oceans.

While the known on-orbit activities of Cosmos 2499, Cosmos 2501, Cosmos 2504, or Cosmos 2521 did not include explicit testing of offensive capabilities or aggressive maneuvers, it is possible that the technologies they tested could be used offensively or aggressive in the future. One potential offensive use would be to get a radio-frequency jammer close to a satellite, thereby greatly amplifying its ability to interfere with the satellite's communications. While possible, to date there is no direct public evidence of such systems being tested on orbit by Russia.

The onboard tracking and guidance systems used for rendezvous could be used to try and physically collide with another satellite to damage or destroy it. However, the approach would have to involve much higher relative velocities than Russian RPO satellites have demonstrated to date, and potentially involving higher velocities and distances than what these satellites are capable of. Furthermore, the deliberate maneuvering to create a conjunction with the target satellite would be detectable with existing processes already in place to detect accidental close approaches. Warning time of such a close approach would likely be at least hours (for LEO) or days (for GEO), unless the attacking satellite was already in a very similar orbit.

2.2 - Russian Direct-Ascent ASAT

Assessment

Russia is almost certainly capable of some limited direct-ascent ASAT operations, but likely not yet on a sufficient scale or at sufficient altitude to pose a critical threat to U.S. space assets. Core Russian direct-ascent ASAT capabilities are not yet operational, and those currently in development are not planned to have the capability to threaten targets beyond LEO. Russia appears highly motivated to continue development efforts even where military utility is questionable, due at least in part to bureaucratic pressures.

Specifics

The Russian DA-ASAT capabilities currently consist of three primary programs which have direct or indirect counterspace capabilities:

1. Nudol: a rapidly maturing ground-launched ballistic missile designed to be capable of intercepting targets in LEO;
2. Kontakt: an air-launched interceptor designed to be used against targets in LEO orbits, on a several-year development timeline; and
3. S-500: a next-generation exoatmospheric ballistic missile defense system, still several years from deployment, that may have capabilities against targets in low LEO orbits.

All three have their roots in Soviet-era programs but have been revived or reconstituted in recent years.

A-235 / Nudol

The Soviet missile defense system A-135, first released in June 1978, was developed by the Vympel division of the Tactical Missile Corporation, which oversees Russia's multi-layered missile defense architecture.[114] While the system at the time possessed some dual-use potential for use as an ASAT, it was sharply limited, and has since been eliminated by the retirement of the 51T6 long-range interceptor (SH-11 Gorgon).[115]

Designs for the would-be replacement, the A-235 missile defense system, first surfaced in 1985-1986, though little came of it at the time.[116] In 2010, the PVO (Russian space defense company)

[114] "Комплекс 14Ц033 Нудоль, ракета 14А042 [Complex 14TS033 Nudol rocket 14A042]", *MilitaryRussia.ru*, February 2, 2017, http://militaryrussia.ru/blog/topic-806.html

[115] For an in-depth discussion of the A-135 program as well as its limitations, see: Pavel Podvig, "Did Star Wars Help End the Cold War? Soviet Response to the SDI Program," *Russian Forces*, March 17, 2013, http://russianforces.org/podvig/2013/03/did_star_wars_help_end_the_col.shtml. For a discussion of the current state of Russian BMD, including the implications of retiring Gorgon, see Aleksandr Stukalin, "'Samolet-M' and the Future of Moscow Missile Defense," *Moscow Defense Brief*, 2018, http://www.mdb.cast.ru/.

[116] Keir Giles, "Russian Ballistic Missile Defense: Rhetoric and Reality," U.S. Army War College, June 2015, http://www.dtic.mil/get-tr-doc/pdf?AD=ADA625224.

Almaz-Antey began technical design work based on those initial blueprints and entered prototyping and initial production of various software and hardware components over the next several years.[117] Individual components were tested in 2012[118] and initial non-flight testing of the system as a whole was successfully conducted in 2013.[119]

This program birthed the PL-19 Nudol, a missile which evidence suggests is now being developed for the direct purpose of direct-ascent ASAT operations. Throughout the development process, Almaz-Antey (whose role within the Russian defense complex is development of technologies for "active space defense") has pitched the system as valuable for holding U.S. LEO assets at risk.[120] What little is known publicly about the Nudol flight tests are more suggestive of an orbital ballistic trajectory intercept than a mid-course missile intercept. Most significant, the system itself is described by Russian state-run press reports as a mobile, TEL-based "new Russian long-range missile defense and space defense intercept complex…within the scope of the Nudol OKR [experimental development project]."[121] The system appears to be designated the 14Ts033 (14Ц033), comprised of the 14A042 Nudol rocket, 14P078 command and control system, and 14TS031 radar.[122] There have been six known flight tests, the final four of which were likely successful. Sources suggest that at least the November 2015 test was of just a rocket and did not include a kill vehicle.[123] A report in April 2018, citing unnamed U.S. intelligence officials, stated that the Nudol test in March 2018 was the first time it was fired from the transporter-erector-launcher it will be deployed with.[124] Evidence is inconclusive as to whether any of the remaining tests included a kill vehicle.[125]

---

[117] See "Комплекс 14Ц033 Нудоль, ракета 14А042 [Complex 14033 Nudol, missile 14A042], *MilitaryRussia.ru*, updated February 2, 2017, http://militaryrussia.ru/blog/topic-806.html.

[118] "Годовой отчет Концерна ПВО 'Алмаз-Антей' за 2012 год [Annual Report of the Almaz-Antei Air Defense Concern for 2012]," *LiveJournal*, July 18, 2013, http://saidpvo.livejournal.com/190982.html?page=1.

[119] GSKB Annual Report 2013

[120] "Система ПРО А-235 (ОКР «Нудоль») [PRO-235 System A (OCD "Nudol")]," *Boehhoe Military Review*, May 14,2015, https://topwar.ru/74866-sistema-pro-a-235-okr-nudol.html; 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/.

[121] Bill Gertz, "Russia Just Successfully Tested an Anti-satellite Missile," December 2, 2015, *Business Insider*, http://www.businessinsider.com/russia-just-successfully-tested-an-anti-satellite-missile-2015-12?amp;IR=T&r=UK&IR=T.

[122] Pavel Podvig, "Russia Tests Nudol Anti-Satellite System," *Russian Strategic Nuclear Forces*, April 1, 2016, http://russianforces.org/blog/2016/04/russia_tests_nudol_anti-satell.shtml; Pavel Podvig, "Construction at the Chekhov Radar Site," *Russian Strategic Nuclear Forces*, June 24, 2016, http://russianforces.org/blog/2016/06/construction_at_the_chekhov_radar_site.shtml

[123] Pavel Podvig, "Russia Tests Nudol Anti-Satellite System," *Russian Strategic Nuclear Forces*, April 1, 2016, http://russianforces.org/blog/2016/04/russia_tests_nudol_anti-satell.shtml.

[124] Ankit Panda, "Russia Conducts New Test of 'Nudol' Anti-Satellite System," *The Diplomat*, April 2, 2018, https://thediplomat.com/2018/04/russia-conducts-new-test-of-nudol-anti-satellite-system/.

[125] George Leopold, "Russian Test Reported, But Was it ASAT?," *Defense Systems*, December 22, 2016, https://defensesystems.com/articles/2016/12/22/russian.aspx; L. Todd Wood, "Russia Tests Anti-satellite Weapon," *The Washington Times*, December 21, 2016, http://www.washingtontimes.com/news/2016/dec/21/russia-tests-anti-satellite-weapon-pl-19-nudol/.

Little is known for sure about the operational capabilities of the Nudol, and available estimates for maximum altitude vary widely from approximately 50 km [126] to nearly 1,000 km.[127] Something in the middle but closer to the former is most likely, based on observations from flight tests as well as third-party analysis of suspected components.[128]

Table 2-5 - Nudol flight tests to date

Date	LV	Site	Payload	Apogee
Aug. 12, 2014[129] [failed shortly after launch]	Nudol	??	?	X
Apr. 22, 2015[130] [failed at launch]	Nudol	??	?	X
Nov. 18, 2015[131]	Nudol	Plesetsk[132]	Interceptor KV	200 km?
May 25, 2016[133]	Nudol	Plesetsk	??	100 km?
Dec. 16, 2016[134]	Nudol	"Central Russia" (Plesetsk? Kapustin Yar?)	A-235 Test	100 km?
Mar. 26, 2018	Nudol	Plesetsk		?

Imagery of the Nudol appears to show a mobile launch capability but stationary radar, in keeping with the missile defense application for which it was initially conceived and reports that it relies on the 14TS031 radar system.[135] This has led some experts to note that while the system is movable, without mobile radar, it could be limited to hitting satellites passing over Russian

[126] "#PutinAtWar: New Russian Anti-Ballistic Missile," *Digital Forensic Research Lab*, December 1, 2017, https://medium.com/dfrlab/putinatwar-new-russian-anti-ballistic-missile-4a4194870e0d.

[127] For discussion of conflicting estimates by Russian public sources (ranging from 35km to 850km), whether indicating disagreement, deliberate misinformation, or the existence of multiple interceptors or stages with different capabilities all considered part of the A-235 system see: https://fortunascorner.com/2017/06/27/russia-russias-a-235-nudol-is-an-american-satellite-killer/

[128] See Jonathan McDowell, "Launch Vehicles," Accessed March 21, 2018, http://planet4589.org/space/lvdb/sdb/LV. The suspected apogees were 350km and 500-1000km. These estimates are notably highly consistent with estimates derived by Russian military open source blogger Dimmi from analysis of suspected components and launch observations, which are summarized in a table: "Complex 14TS033," *MilitaryRussia.ru*.

[129] Reported at the time as a failed test of a missile for the Antey-2500 air defense system. See "Концерн «Алмаз-Антей» проводил на космодроме Плесецк испытания модернизированной ракеты [Concern Almaz-Antey conducted tests of a modernized rocket at the Plesetsk cosmodrome], *Kommersant.ru*, August 12, 2014, https://www.kommersant.ru/doc/2714669.

[130] Pavel Podvig, "Dates of Nudol ASAT Tests," *Russian Strategic Nuclear Forces,* May 10, 2016, http://russianforces.org/blog/2016/05/dates_of_nudol_asat_tests.shtml.

[131] Jonathan McDowell, "Jonathan's Space Report No. 720," December 16, 2015, http://www.planet4589.org/pipermail/jsr/2015-December/000092.html.

[132] Pavel Podvig, "Russia Tests Nudol Anti-Satellite System," *Russian Strategic Nuclear Forces*, April 1, 2016, http://russianforces.org/blog/2016/04/russia_tests_nudol_anti-satell.shtml.

[133] Gertz, Bill, "Russia Flight Tests Anti-Satellite Missile," *The Washington Free* Beacon, May 27, 2016, http://freebeacon.com/national-security/russia-flight-tests-anti-satellite-missile; Jonathan McDowell, "Jonathan's Space Report, No. 726," May 30, 2016, http://www.planet4589.org/pipermail/jsr/2016-May/000098.html.

[134] Ibid.

[135] "Противоракеты [Anti-Missile Systems]," *LiveJounral.com*, January 17, 2015, http://bmpd.livejournal.com/1137442.html.

territory.[136] However, several factors reduce the salience of this fact. First, in the event of a conflict in Russia's near abroad, many of the most relevant U.S. assets would indeed be passing overhead. More importantly, Russia is rapidly maturing multiple technologies for advanced targeting, tracking, and measurement. These include, among others: ground-based lasers which, while stationary, are a more flexible means of target-acquisition than radar; mobile radar; space-based targeting, tracking, and measurement (TT&M) and SSA capabilities; expansion and modernization of ground-based space monitoring sites throughout Russia; and on-board guidance systems akin to those employed for late-stage course-correction of conventional and nuclear cruise and ballistic missiles.[137]

Figure 5 -TEL-mounted Nudol
Artist's depiction from company calendar.
Image credit: Almaz-Antey.[138]

It is possible that nuclear-arming of the Nudol under at least some circumstances is being considered, but the evidence is not conclusive. Available depictions of the Nudol TEL has features

[136] Gertz, Bill, "Russia Flight Tests Anti-Satellite Missile," *The Washington Free* Beacon, May 27, 2016, http://freebeacon.com/national-security/russia-flight-tests-anti-satellite-missile.
[137] A number of on-board and ground complex systems being developed and upgraded for use with the Nudol in particular, including a new final-stage interceptor guidance and control system, a dedicated next-generation radar beginning with the 14TS031 radar with digital adaptive phased array, new hardware and software specially developed by A/A for ground command of the Nudol, planned integration with a more comprehensive space- and ground-based early warning system, and a specially-upgraded version of the "Don-2N"/5N20 and "Don-2NP"/5N20P radar systems in the interim. See: "Complex 14TS033," MilitaryRussia.ru.
[138] "Противоракеты [Anti-Missile Systems]," LiveJounral.com, January 17, 2015, http://bmpd.livejournal.com/1137442.html.

that appear to be environmental control systems (ECS) on the missile tubes—a feature typically associated with nuclear-armed missiles.[139] And there is precedent for such a decision: the 51T6 Gorgon was nuclear-tipped due to persistent skepticism regarding the efficacy and reliability of non-nuclear missile defense.[140] Some Soviet and Russian military strategists have discussed the desirability of nuclear ASATs for reliable, rapid, and wide-area kinetic and EMP effect, but there is no conclusive public evidence that the Soviet Union or Russia planned on nuclear-tipped ASAT weapons, even as part of their response to Reagan's Strategic Defense Initiative (SDI).[141] There are also some who argue that Russia has shifted its nuclear doctrine towards the use of tactical nuclear weapons for warfighting, but most Russian experts conclude that this has not yet happened.[142] Moreover, Russian-language media reported in early 2018 that the system would not be equipped with nuclear warheads.[143] Deployment is reportedly scheduled for late 2018.[144]

78M6 Kontakt

The second category of direct-ascent ASAT system explored by the Soviet Union, and seemingly resurrected in recent years, is an air-launched missile system known as Kontakt. The launch platform was originally intended to be a variant of the MiG-31 'Foxhound', designated the MiG-31D.[145] At least six such aircraft were completed in the 1980s, with intent to be fitted with a Vympel-developed ASAT missile dubbed the 79M6 "Kontakt".[146] Two waves of interceptor development were planned in the 1980s: the first was to be a three-stage interceptor capable of hitting targets at orbits of 120-600 km; the second was to reach altitudes of up to 1,500 km.[147] The system was also intended to be capable of deploying with little or no warning, in contrast to the

---

[139] Note that this, while a decent indicator, is not definitive: an alternative possibility is that the ECS components are present to protect the seeker/kill vehicle, or that the image was manipulated by the employees at Almaz-Antey responsible for producing it prior to publication.

[140] Sean O'Connor, "Russian/Soviet Anti-Ballistic Missile Systems," *Air Power Australia*, January 27, 2014, http://www.ausairpower.net/APA-Rus-ABM-Systems.html#mozTocId371125; Pavel Podvig, (ed.), 2001, *Russian strategic nuclear forces*, Cambridge, MA: MIT Press, p. 416; Laura Grego, "A History of Anti-Satellite Programs," *Union of Concerned Scientists*, January 2012, https://www.ucsusa.org/sites/default/files/legacy/assets/documents/nwgs/a-history-of-ASAT-programs_lo-res.pdf.

[141] Pavel Podvig, "Did Star Wars Help End the Cold War? Soviet Response to the SDI Program," *Russian Forces*, March 17, 2013, http://russianforces.org/podvig/2013/03/did_star_wars_help_end_the_col.shtml.

[142] Olga Oliker and Andrey Baklitskiy, "The Nuclear Posture Review and Russian 'De-Descalaton:' A Dangerous Solution to a Nonexistent Problem," *War on the Rocks*, February 20, 2018, https://warontherocks.com/2018/02/nuclear-posture-review-russian-de-escalation-dangerous-solution-nonexistent-problem.

[143] Nikolay Surkov and Alexey Ramm, "Москва получит новую противоракетную защиту [Moscow will receive a new anti-missile defense]," *Izvestia*, February 21, 2018, https://iz.ru/710845/nikolai-surkov-aleksei-ramm/moskva-poluchit-novuiu-protivoraketnuiu-zashchitu.

[144] "СМИ: в Москве усилят систему ПРО [Media: Moscow to strengthen missile defense system]," *Gazeta.ru*, February 21, 2018, https://www.gazeta.ru/army/news/11195629.shtml.

[145] "MiG-31 Foxhound Interceptor Aircraft," *AirForce-Technology.com*, accessed March 15, 2018, http://www.airforce-technology.com/projects/mig-31/; "Russians Alter MiG-31 for ASAT Carrier Roles," *Aviation Week and Space Technology*, 17 August 1992, p.63. For a fully comprehensive treatment of the aircraft and its variants, see: Yefim Gordon, *MiG-25 Foxbat, MiG-31 Foxhound: Russia's Defensive Front Line*, Midland Publishing Ltd. (England), 1997. For a concise but detailed description of the MiG-31D, including its design specifications, differences from the standard MiG-31, and method of ASAT operation, refer to John Pike, "USSR/CIS Miniature ASAT," *GlobalSecurity.org*, updated October 4, 2016, http://www.globalsecurity.org/space/world/russia/mini.htm.

[146] Ibid.

[147] Pavel Podvig, "Another Old Anti-satellite System Resurfaces," *Russian Strategic Nuclear Forces*, January 25, 2013, http://russianforces.org/blog/2013/01/another_old_anti-satellite_sys.shtml.

USSR's co-orbital interceptors,[148] and of attacking large numbers of satellites quickly: Soviet documents speak of an operational target of at least 24 satellites within 36 hours, or as many as 20-40 satellites within 24 hours.[149]

The program was based out of Sary Shagan with support to be provided by the Krona optical space surveillance complex, and allegedly became ready for flight-testing around 1991.[150] Whether such testing ever actually occurred has been an open question, with the program remaining shrouded in secrecy, but recent reports from a former MiG test pilot describe several tests in which the missile was successfully launched from a MiG-31D in flight, homed in on a Soviet target, and then did a deliberate near-miss before self-detonating to prevent Americans from discovering the program.[151] If true, this would demonstrate maturity of the rocket (likely retained to the present day as other such assets were), but also of the aircraft's special upward-facing radar array, ground-based targeting and command-and-control complexes, and ability to stably and accurately launch at-speed.

Put on hold due to budget cuts in the 1990s, the program was officially resumed by the Russian Air Force in 2009.[152] Little public evidence exists that would confirm the existence, much less operational nature, of a viable air-launched ASAT at-present, but both the launch platform and ground-based support systems are undergoing intensive modernization efforts. A version of the launch platform nominally geared toward small satellite payloads rather than a direct-ascent interceptor was pursued, dubbed the MiG-31S, and successfully tested.[153] Another variant, designated the MiG-31FE and proposed for export to China and India as early as 1995, was intended to be sold in conjunction with an arms package of two very long-range missiles able to intercept ballistic missiles at altitudes of 200 km and speeds of up to Mach 20.[154] A modernized version of the MiG-31BM has since been acquired and deployed, which is capable of tracking and destroying multiple simultaneous targets at ranges of 320 km at high speed.[155] Russia has also retained at least two of the original MiG-31D ASAT variant, stationed in Kazakhstan, and uses one of them to conduct near-space flights for hypersonic experimentation, most likely the recently-

[148] John Pike, "USSR/CIS Miniature ASAT," *GlobalSecurity.org*, updated October 4, 2016, http://www.globalsecurity.org/space/world/russia/mini.htm.
[149] Pavel Podvig, "Another Old Anti-satellite System Resurfaces," *Russian Strategic Nuclear Forces*, January 25, 2013, http://russianforces.org/blog/2013/01/another_old_anti-satellite_sys.shtml.
[150] Anatoly Zak, "Anti-Satellite Weapons: History and Definitions," presentation given at a United Nations Institute for Disarmament Research conference, March 2014, http://www.unidir.ch/files/conferences/pdfs/anti-satellite-weapons-asats-history-and-definitions-en-1-968.pdf.
[151] Audio of the interview with MiG test pilot Valery Menitsky is available here (accessed 12 July 2017): http://www.buran.ru/sound/men_31d.mp3.
[152] Anatoly Zak, "Anti-Satellite Weapons: History and Definitions," presentation given at a United Nations Institute for Disarmament Research conference, March 2014, http://www.unidir.ch/files/conferences/pdfs/anti-satellite-weapons-asats-history-and-definitions-en-1-968.pdf.
[153] John Pike, "USSR/CIS Miniature ASAT," *GlobalSecurity.org*, updated October 4, 2016, http://www.globalsecurity.org/space/world/russia/mini.htm.
[154] John Pike, "MiG-31BM (Bolshaya Modernizatsiya - Big Modernization)," *GlobalSecurity.org*, updated November 4, 2015, http://www.globalsecurity.org/military/world/russia/mig-31bm.htm .
[155] Ibid.

announced Kinzhal air-launched cruise missile.[156] If so, that may indicate they are no longer slated for use with ASAT weapons.

Meanwhile, the integrated detection, targeting, tracking, and communications networks on which an airborne DA-ASAT system would depend are being expanded and new facilities constructed: a new Krona ground radar-optical complex was recently constructed at Nakhodka (See Russian Space surveillance complexes; Section 8-20), a total of three others have been built over time (one each at Stavropolye, Сары-Шаган, and near Moscow), and all have undergone significant and ongoing technological upgrades in recent years.[157] These upgrades have been followed by testing which, according to Russian military officials, has featured a particular emphasis on "interaction of various components, especially the impact means, with a ground-radar optical complex search and identification of artificial satellites" in order to "deal with the satellites."[158] In November 2017, the Deputy Head of 46th TsNII research institute of the Ministry of Defense, Oleg Ochasov, notified the Russian parliament that the 2018-2027 Russian federal defense procurement program would allocate funding for development of the "Rudolph mobile anti-satellite complex."[159]

It is possible that Russia is working to bring the Kontakt capability online in the near future.[160] In early 2017, a commander in the VKF informed the media that Russia plans to deploy an ASAT missile aboard the MiG-31BM, an additional high-altitude air-to-air interceptor variant of the Foxhound, claiming that "a new missile is being developed for this aircraft capable of destroying targets in near-space….Satellites, for sure…".[161] This claim is unconfirmed, and some experts have expressed doubt due to the lack of image or serial number confirmation of a model carrying an ASAT missile, and because the MiG-31BM lacks the special winglets present on the MiG-31D for enhanced high-altitude launch stability.[162] However, several Russian air-launched ASAT concepts also do not include such winglets, nor does a two aircraft MiG-31 variant produced in conjunction with Kazakhstan for in-air space-launch operations and hypersonic experimentation, so this fact is hardly damning.[163] This coincides with unconfirmed but plausible rumors, bolstered

[156] John Pike, "USSR/CIS Miniature ASAT," *GlobalSecurity.org*, updated October 4, 2016, http://www.globalsecurity.org/space/world/russia/mini.htm.
[157] "СМИ: Минобороны готовится испытать противоспутниковый комплекс [Media: the Ministry of Defense is preparing to test the anti-complex]," Vzyglad, 24 January 2013, https://vz.ru/news/2013/1/24/617307.html; Dmitriy Balburov, and Aleksei Mikhailov, "Tests of Antisatellite Complex Will Begin at the End of the Year: Revived Soviet Krona Will Down Satellites With Ground-Based or Air-Launched Missiles," *Izvestia*, January 24, 2013.
[158] "СМИ: Минобороны готовится испытать противоспутниковый комплекс [Media: the Ministry of Defense is preparing to test the anti-complex]," Vzyglad, 24 January 2013, https://vz.ru/news/2013/1/24/617307.html
[159] Anatoly Zak, "Russian Anti-Satellite Systems," *Russian Space Web*, updated November 30, 2017, http://www.russianspaceweb.com/naryad.html.
[160] Daniel Coats, "Worldwide Threat Assessment of the U.S. Intelligence Community," unclassified statement for the record before the Senate Select Committee on Intelligence, May 11, 2017, https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf.
[161] Alexander Zudin, "Russia to Deploy Anti-Satellite Weapon on MiG-31BM", *Jane's 360*, February 23, 2017, http://www.janes.com/article/68102/russia-to-deploy-anti-satellite-weapon-on-mig-31bm.htm
[162] Twitter discussion between Pavel Podvig, "KURYER" (curator of militaryrussia.ru, @RSS_40), Thomas Newdick (@CombatAir), and Wolfgang Dressler (@dressler_w), February 23-24 2017, https://twitter.com/rss_40/status/835012292337098753?lang=en.
[163] Ibid.

by leaked partial images of design concepts, that a new interceptor to replace the Kontakt is being developed at Fakel.[164]

S-500 ABM

Moscow is also developing next-generation missile defense capabilities, the most advanced of which is the S-500 anti-ballistic missile (ABM) system.[165] Relatively little information about the S-500 exists in the public domain, but it appears to include an exoatmospheric interceptor, capable of destroying not only ballistic missiles prior to re-entry but also objects in orbit.[166] Russian officials, in the years following the Chinese and U.S. ASAT and missile defense tests of the late 2000s, began to explicitly discuss the S-500 as serving a dual missile defense-ASAT purpose.[167] The development of dedicated ASATs since then, however, makes this less likely. The system was originally intended to begin production and deployment in 2016 or 2017,[168] but had not yet completed testing.[169] Russian media report that the S-500 entered production in March 2018, with the system being manufactured at the Almaz-Antey plant in Nizhny Novgorod and missiles in Kirov.[170] Russian defense minister Sergei Shoigu has announced that he expects deliveries to begin as soon as 2020, and funding has been guaranteed as part of the State Armament Program 2018-2027;[171] Russia reportedly planned to field ten battalions of the new system at latest estimate.[172]

Potential Military Utility

Given the known testing, it is likely that Russia has some existing capability to field an operational DA-ASAT capability against most LEO satellites within the next few years. This would include satellites performing military weather and ISR functions. Russia would have to wait for such satellites to overfly an area where one of the systems is deployed, but most LEO satellites would do so daily to every few days. However, once launched, the target would only have an estimated 8-15 minutes warning time before impact. Moreover, the potential for an air-launched DA-ASAT capability could dramatically expand the potential launch opportunities.

---

[164] "Russian Military Future Space Projects," *DefenceTalk Forum*, January 24, 2013, http://www.defencetalk.com/forums/space-defense-technology/russian-military-future-space-projects-12386/.
[165] Sebastien Roblin, "Russia's S-500: The Ultimate Weapon Against American Missiles or a Paper Tiger?," *The National Interest*, November 4, 2016, http://nationalinterest.org/blog/the-buzz/russias-s-500-the-ultimate-weapons-against-american-missiles-18294.
[166] Christopher F. Foss, "S-500," *Jane's Land Warfare Platforms: Artillery and Air Defense* (London: IHS Global, 2016), 580-1; Bill Gertz, "Pentagon: China, Russia Soon Capable of Destroying U.S. Satellites," *The Washington Free Beacon*, January 30, 2018, http://freebeacon.com/national-security/pentagon-china-russia-soon-capable-destroying-u-s-satellites/.
[167] Anatoly Zak, "Russian Anti-Satellite Systems," *Russian Space Web*, updated November 30, 2017, http://www.russianspaceweb.com/naryad.html.
[168] Brendan McGarry, "Russia Still Developing S-500 Surface-to-Air Missile Systems: Analyst," *Defensetech.com*, July 19, 2016, https://www.defensetech.org/2016/07/19/russia-still-developing-s-500-surface-to-air-missiles/; "S-500 Prometheus," *Missile Threat*, updated May 4, 2017, https://missilethreat.csis.org/defsys/s-500-prometheus/.
[169] Ibid.
[170] Vladimir Karnozov, "Russia's Next-generation S-500 SAM Enters Production," *AINonline*, March 14, 2018, https://www.ainonline.com/aviation-news/defense/2018-03-14/russias-next-generation-s-500-sam-enters-production.
[171] Ibid.
[172] Andrius Genys, "S-500," *Military Today*, April 5, 2017, http://www.military-today.com/missiles/s500.htm.

To date, there is no public evidence suggesting Russia is experimenting with or developing DA-ASAT capabilities against satellites in higher orbits such as MEO or GEO.

At the same time, there are also constraints on the military utility of such systems, particularly as Russia replenishes its own space capabilities. The use of a kinetic-kill DA-ASAT against an orbital target will invariably create large amounts of orbital space debris, as was seen in the 2007 Chinese ASAT test. An aggressive use of such a capability would invariably lead to widespread condemnation, as happened after the 2007 Chinese ASAT test. The debris will pose just as much a threat to Russia's space capabilities, including its human spaceflight program, as it does those of other countries. Thus, the military utility of DA-ASATs would have to be weighed against the potential costs, particularly relative to less destructive capabilities such as jamming or blinding. Use of a DA-ASAT would also be relatively easy to attribute to Russia.

2.3 - Russian Electronic Warfare

Assessment

Russia places a high priority on integrating electronic warfare (EW) into military operations and has been investing heavily in modernizing this capability. Most of the upgrades have focused on multifunction tactical systems whose counterspace capability is limited to jamming of user terminals within tactical ranges. Russia has a multitude of systems that can jam GPS receivers within a local area, potentially interfering with the guidance systems of unmanned aerial vehicles (UAVs), guided missiles, and precision guided munitions, but has no publicly known capability to interfere with the GPS satellites themselves using radiofrequency (RF) interference. The Russian Army fields several types of mobile EW systems, some of which can jam specific satellite communications user terminals within tactical ranges. Russia can likely jam communications satellites uplinks over a wide area from fixed ground stations. Russia has operational experience in the use of counterspace EW capabilities from recent military campaigns.

Specifics

Electronic warfare is defined as "military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy."[173] In the context of this report, the scope of EW is narrowed to refer specifically to intentional interference with an adversary's radiofrequency transmissions to or from a satellite. This intentional interference is often referred to as "jamming".[174]

In the case of satellite signals, jamming is often characterized as being either uplink or downlink. Uplink, or orbital, jamming occurs when an interference signal targets the satellite directly. Most communication satellites serve as a relay node that rebroadcast signals directed at it, or uplinked, from the ground. The uplink interference signal can originate anywhere within the satellite receive antenna beam and overwhelms the intended signal such that the signal re-transmitted by the satellite and received by the users on the ground consists of indecipherable noise. The impact may be widespread since all users within the satellite's service area (known as the footprint) are affected. Downlink, or terrestrial, jamming targets the ground user of satellite services, by broadcasting a RF signal that overwhelms the intended satellite signal for users in a specific area. In downlink jamming, the satellite itself suffers no interference, nor would users outside the range of the jammer.

[173] United States Department of Defense, "DOD Dictionary of Military and Associated Terms," *Defense Technical Information Center*, February 2018, pg. 78, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.
[174] Ibid, pg. 76.

Figure 6 - Uplink vs downlink jamming
Image credit: Infosec Institute.[175]

Modern militaries regard EW capabilities and vulnerabilities as highly sensitive information and hence little public information is generally available. Development and testing of equipment and techniques can be conducted within secure defense facilities, leaving little or no external evidence of the activities. Given the paucity of public information on EW in general, and Russian counterspace EW in particular, this assessment relies, in part, on indirect evidence, principally Russian technological capability, EW doctrine and known EW capabilities in other environments.[176]

The three principal areas of concern with regards to Russia are the jamming of:

1. Global navigation satellite systems (GNSS) signals
2. Satellite communications
3. Synthetic aperture radar (SAR) imaging

GNSS Jamming

GNSS jamming, particularly of the U.S. GPS, is a well-known technology and jammers are widely proliferated throughout the globe. Russia is assessed to be very proficient in GPS jamming capabilities, having developed both fixed and mobile systems. The known systems are downlink

[175] Pierluigi Paganini,"Hacking Satellites: Look Up To the Sky," *Infosec Institute*, September 18, 2013, http://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/#gref.
[176] Laurie Moe Buckhout, "Modern Russian Electronic Warfare," *SITREP Quarterly Review of C4ISR Technology Advancements*, Q1 2016, http://www.leonardodrs.com/sitrep/q1-2016-the-invisible-fight/modern-russian-electronic-warfare/.

jammers, which affect GPS receivers within a local area. There is no known system that targets uplink jamming of the GPS satellites themselves.

The first category of Russian GPS jammers are used to protect fixed facilities. For example, Russian state media announced that Russia is deploying 250,000 GPS jammers on cell phone towers throughout the country. [177] The objective of these Pole-21" jammers, developed by the JSC Scientific and Technical Center of Electronic Warfare is to reduce the accuracy of foreign UAVs and cruise missiles over much of the Russian land mass, thereby protecting fixed installations. The Pole-21 systems are reported to be effective to a range of 80 km.[178]

The second category of Russian GPS jammers are mobile systems that are integrated within military EW units and form a critical component of Russian military capabilities. [179] These units are equipped with multifunction EW equipment, a number of which have GPS jamming capability. Two of these are the R-330Zh "Zhitel" and the "Borisoglebsk-2".[180] [181] The role of these systems is to protect Russian units by jamming an adversary's tactical signals. The local jamming of GPS seeks to negate the effectiveness of UAVs, cruise missiles and precision guided munitions (PGMs). Recently, there have been multiple reports of Russia deploying some of these EW systems in support of Russian deployments in Syria and Ukraine. [182] [183] [184]

[177] 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," *The Next Big Future*, October 18, 2016, https://www.nextbigfuture.com/2016/10/russia-will-place-gps-jammers-on-250000.html.
[178] "Silent Protector: Russia Develops Hi-Tech Jammer to Block Enemy Electronics," *Sputnik International*, August 25, 2016, https://sputniknews.com/russia/201608251044633778-russia-jammer-electronics/.
[179] "Electronic Warfare Chief Interviewed," *Russian Defense Policy,* May 30 2017, https://russiandefpolicy.blog/tag/electronic-warfare/.
[180] "R330ZH," *Rosobornexport*, accessed March 15, 2018, http://roe.ru/eng/catalog/air-defence-systems/elint-and-ew-equipment/r-33ozh/.
[181] "Sky's the Limit: Russia's Unique Jamming System Getting Upgrade," *Sputnik News*, May 12, 2016, https://sputniknews.com/russia/201612051048187517-russia-electronic-warfare-system/.
[182] 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.
[183] "It is Official, Russian Army Deployed R-330Zh Jammer in the Battle of Debaltseve," *Inform Napalm*, April 23, 2016, https://informnapalm.org/en/r-330zh-jammer-battle-debaltseve/.
[184] Sergey Sukhankin, "Russian Electronic Warfare in Ukraine: Between Real and Imaginable," *Real Clear Defense* May 26, 2017, https://www.realcleardefense.com/articles/2017/05/26/russian_electronic_warfare_in_ukraine_111460.html.

Figure 7 - R-330ZH and Borisoglebsk-2

Image credits: Inform Napalm[185] and topwar.ru.[186]

There have also been reports of GPS interference occurring outside of conflict zones. In June 2017, the captain of a tanker approaching the Russian Black Sea port of Novorossiysk noticed a sudden anomaly in the ship's GPS system, placing its location approximately 30 miles away on land near the local airport. Additionally, the Automated Identification System (AIS), a navigation safety communication system carried by all large commercial ships, reported that a number of other ships were also located near the airport. The AIS system relies on GPS to identify a ship's location. This anomaly could have been caused by GPS spoofing exercises or tests conducted by the Russian military, likely within the parameters of a test program or exercise in the local area and the ships were unintentionally affected. [187]

No Russian system is known to be capable of targeting the GPS satellites themselves (uplink jamming).

Jamming of Communications Satellites

There is virtually no reliable public information source regarding Russian capabilities to uplink jam communications satellites. No specific incidents have been reported, official sources have not commented on capabilities, and no equipment or facilities have been publicly identified. However, this is not to be considered unusual, and does not mean Russia has not developed these capabilities. As previously stated, electronic warfare is a highly classified component of most militaries and capabilities are seldom revealed. The equipment and facilities necessary for jamming of satellite communications have no unique characteristics that would distinguish them from standard satellite

[185] "It is Official, Russian Army Deployed R-330Zh Jammer in the Battle of Debaltseve," *Inform Napalm*, April 23, 2016, https://informnapalm.org/en/r-330zh-jammer-battle-debaltseve/.
[186] Sergey Sukhankin, "Russia Tests EW Capabilities Ahead of Zapad 2017," *Eurasia Daily Monitor*, Volume: 14 Issue: 108, September 8, 2017, https://jamestown.org/program/russia-tests-ew-capabilities-ahead-of-zapad-2017/.
[187] Matt Burgess, "When a Tanker Vanishes, All the Evidence Points to Russia," *Wired*, September 21, 2017, https://www.wired.co.uk/article/black-sea-ship-hacking-russia.

communications uplink facilities. The primary differences would not be observable: output power, waveforms and processing equipment. Thus, satellite uplink stations of all types could easily be adapted for jamming.

Russia has also committed to develop more advanced EW and communications jamming capabilities over the next decade. In November 2017, Oleg Ochasov, the Deputy Head of 46th TsNII research institute of the Ministry of Defense, disclosed to the Russian parliament in connection with the 2018-2027 defense procurement program that the "Tirada-2S electronic warfare complex…specialized in jamming communications satellites" was under development, and "expected to be available in 'ground' and 'mobile' architectures."[188]

We assess that Russia has a robust capability to jam uplinks to communications satellites from fixed sites, although the identifications of these sites are not known. The assessment is based, not on hard evidence of use or testing, but on technological capability and EW doctrine.

In contrast, Russian tactical systems are reported to have the capability to perform local downlink jamming of some communication satellite frequencies. One example is the R-330Zh "Zhitel" which is reportedly able to jam commercial INMARSAT and Iridium receivers within a tactical local area.

Jamming of SAR Satellites

The Krashukha-4 mobile electronic warfare system, manufactured by Russia's Radio-Electronic Technologies Group (KRET), is designed to counter airborne early warning and control systems (AWACS) and other airborne radar. Due to its range and power, it is also reported to be effective against LEO synthetic aperture radar imaging satellites.[189] There is no reliable public documentation suggesting that systems for RF jamming from orbit are in existence, being developed or researched by Russia.

[188] Anatoly Zak, "Russian Anti-Satellite Systems," *Russian Space Web*, November 30, 2017, http://www.russianspaceweb.com/naryad.html.
[189] "Jamming the Enemy: Russia Ramps Up Production of Electronic Warfare Systems," *Sputnik News*, May 13, 2017, https://sputniknews.com/military/201705131053579633-russia-electronic-warfare-systems-production/.

Figure 8 - Krasukha-4
A Russian mobile electronic warfare system used to jam radar.
Image credit: Sputnik News.[190]

Potential Military Utility

RF jamming is an effective means of negating certain space capabilities. The most significant and prevalent, thus far, is using EW to degrade the accuracy of GPS-guided systems in tactical scenarios. Given this high reliance of modern militaries on GNSS, and GPS in particular, Russia is likely to yield significant military utility from being able to actively prevent, or even undermine confidence in, the ability of adversaries to use GNSS in a future conflict.

EW can be used to suppress or degrade space capabilities by means of uplink jamming of communications satellites. It is an attractive option for counterspace because of its flexibility: it can be temporarily applied, its effects on a satellite are completely reversible, it generates no on-orbit debris, and it may be narrowly targeted, which could affect only one of a satellite's many capabilities (e.g. specific frequencies or transponders). EW is an extremely useful military counterspace capability and is expected to gain even more prominence in the future, in step with increasing autonomy of military systems and increasing reliance on satellite systems.

[190] "Invisible Shield, Invisible Sword: Russia's Electronic Warfare 'Second to None'," *Sputnik News*, August 31, 2017, https://sputniknews.com/military/201708311056962045-russia-electronic-warfare-system-krasukha/.

2.4 - Russian Directed Energy Weapons

Assessment

Russia has a strong technological knowledge base in directed energy physics and is developing a number of military applications for laser systems in a variety of environments. Russia has revived, and continues to evolve, a legacy program whose goal is to develop an aircraft-borne laser system for targeting the optical sensors of imagery reconnaissance satellites, although there is no conclusive evidence that an operational capability has been achieved.

Although not their intended purpose, Russian ground-based satellite laser ranging (SLR) facilities could be used to dazzle the sensors of optical imagery satellites.

There is no indication that Russia is developing, or intending to develop, high power space-based laser weapons.

Specifics

The use of lasers in satellite countermeasure or weapon applications can be classed into three categories based on their effects:

1. Dazzling of a satellite's imaging sensor
2. Damage to a satellite's image sensor
3. Damage of the satellite bus or its subsystems

Laser dazzling is more appropriately considered a countermeasure than a weapon, since the effect is not permanent. The dazzling phenomenon consists of directing a relatively low power laser beam into the optics of an imaging satellite. The laser light will impinge on the sensors detector array - usually a charge-coupled device (CCD) or a complementary metal-oxide semiconductor (CMOS) - and overwhelm the natural collection of photons. As a result, a number of the pixels of an image will be saturated, thus obscuring a portion of the image scene. The effects may persist in the sensor and associated electronics would be temporary in nature. For example, in a CCD array, it might take several successive readouts of the array in order to completely clear the electric charge that was induced by the laser. Therefore, the effect may impact a number of images, following the laser incident. However, this effect is considered to be temporary in nature since it will eventually clear on its own with no operator intervention. Laser dazzling could be used as a countermeasure in order to protect specific ground facilities from being imaged by optical means. The laser source would need to be located near the target it is intended to protect.[191]

[191] David Wright, Laura Grego, and Lisbeth Gronlund, *The Physics of Space Security*, American Academy of Arts and Science, 2005, Appendix A to Section 11, http://www.ucsusa.org/sites/default/files/legacy/assets/documents/nwgs/physics-space-security.pdf.

Since imaging sensors are very sensitive to light, relatively low power levels are required to dazzle. For example, Satellite Laser Ranging (SLR) is a mechanism to accurately track satellites that have been equipped with laser retro reflectors. SLR is used for satellites in which the precise knowledge of position and orbits is essential for their mission (e.g. geodetic or navigation satellites). Low power lasers used for SLR would be of sufficient power to dazzle imaging sensors. The amount of power required to dazzle but not damage is not clear and depends on several factors specific to the particular situation. Factors relating to wavelength, atmospheric conditions and, in particular, the design of the satellite optics and sensor all contribute. However, rough estimates suggest that even a 10 W laser could be sufficient to create a dazzling effect and obscure an area on the ground.[192] Ultimately the most difficult aspect of laser dazzling is not the power of the laser, but accurate tracking of the satellite.

Damage to a satellite's image sensor, or associated electronics, could be caused when the laser power is of sufficient intensity. Damage to optics would involve a higher power than dazzling. However, the threshold between dazzling and damage is almost impossible to predict; thus, whenever a dazzling attempt is made there may be a risk of damage. This is because the ground area obscured (corresponding to the portion of the sensor dazzled) increases with increasing laser power. At the high end, where a large portion of the array becomes saturated, some of the sensor elements may become subject to sufficient intensity to cause permanent damage. Under some conditions, damage to a portion of the sensor array could be incurred using a continuous wave with a power level as low 40 W. This power level would likely only affect a few pixels in the array, but it would be permanent damage nonetheless. A more likely power level to use for a weapons application where significant damage to the sensor was intended would be in the KW range.[193]

In the case of damage to optical sensors, the satellite will not otherwise be damaged. It can continue to be controlled and operate and the other non-imaging payloads will continue to function.

Damage to the satellite bus could be inflicted with the use of a very high-power laser. The damage would be due to the thermal effects of the absorbed energy causing failure of some essential components of the bus (ex. thermal regulation system, the batteries, or attitude control system). In this scenario, there is a complete failure of the satellite. All satellites would be potentially susceptible to this type of attack, but it would require a large very high-power laser system.

Russia is has a long history of research in high-energy laser physics science and is considered to have advanced technical knowledge and capability in this field. During the 1980s, the USSR reportedly researched several potential anti-satellite laser weapon systems, although there is no evidence that any reached the stage of realistic testing or deployment.[194] With the economic

[192] Ibid.
[193] Ibid.
[194] John Pike, "Lasers," *GlobalSecurity.Org*, updated October 4, 2016, https://www.globalsecurity.org/space/world/russia/lasers.htm.

turmoil created by the dissolution of the USSR, these programs appear to have been abandoned. However, the scientific knowledge base remained.

The resurgence of Russia in the past decade enabled increased funding for military research, which in turn allowed continued Russian research into advanced laser technologies and applications. For example, it was recently reported that Institute of Atmospheric Optics at Tomsk has developed a laser system with the capability to shoot down drones, using fiber laser technology.[195] This system would, however, have no capability against spacecraft in orbit.

Airborne Laser (ABL) ASAT System

During the 1980s, the USSR began a development program to mount a high-power laser on a modified IL-76 transport aircraft (known as the Beriev A-60). The laser was installed in the cargo bay, with a turret opening on the top of the aircraft. The aircraft was used to test the laser system that was later used in the Skif-DM spacecraft, lost in a failed launch in 1987. The test aircraft was reportedly lost in a fire during the late 1980s. A second aircraft was modified for continued testing. In 2009, the aircraft laser reportedly conducted a successful test of illuminating a satellite in orbit. Work on the project was halted in 2011, due to lack of funding.[196]

In 2012, the Ministry of Defense announced the revival of the program.[197] In April 2017, Almaz-Antey general designer Pavel Sozinov announced that the company had been ordered by Russian leadership to "develop weapons that could interfere electronically with or achieve 'direct functional destruction of those elements deployed in orbit.'"[198] The new system, called "Falcon Echelon," will be equipped with the 1LK222 laser system, apparently a different system than the original Carbon Dioxide laser type from the 1980s. The new laser will reportedly be fitted aboard a "brand-new, as-yet-unnamed" aircraft, according to recent Russian media reports.[199]

There is no public technical information available on the 1LK222 laser system. It is therefore not possible to determine if its mission is to dazzle or to damage satellite sensors. If the 1KL222 is a solid-state laser, it could be operated at different power levels, thereby making it possible to operate in both laser dazzling and optical sensor damage roles. Due to the technical challenges of operation on an aircraft, it is unlikely that that the laser is sufficiently high powered to cause damage to a satellite's structure. Therefore, it is likely intended to target only optical imaging

---

[195] "Russian Scientists Invent Technology to Wirelessly Recharge and 'Kill' Drones," *Russian Aviation*, June 21, 2017, https://www.ruaviation.com/news/2017/6/21/9042/?h.
[196] John Pike, "A-60 1A Airborne Laser," *GlobalSecurity.org*, August 3, 2018, https://www.globalsecurity.org/military/world/russia/a-60.htm.
[197] Pavel Podvig, "Russia to Resume Work on Airborne Laser ASAT," *Russian Strategic Nuclear Forces*, November 13, 2012, http://russianforces.org/blog/2012/11/russia_to_resume_work_on_airbo.shtml.
[198] Patrick Tucker, "Russia Claims It Now Has Lasers to Shoot Satellites," *Defense One*, February 26, 2018, http://www.defenseone.com/technology/2018/02/russia-claims-it-now-has-lasers-shoot-satellites/146243/; "В РФ разрабатывается противоспутниковая система РЭБ," *Ria Novosti*, April 25, 2017, https://topwar.ru/114285-v-rf-razrabatyvaetsya-protivosputnikovaya-sistema-reb.html.
[199] Patrick Tucker, "Russia Claims It Now Has Lasers to Shoot Satellites," *Defense One*, February 26, 2018, http://www.defenseone.com/technology/2018/02/russia-claims-it-now-has-lasers-shoot-satellites/146243/.

satellites. An airborne system provides a few advantages for laser ASAT systems. The high flight altitude reduces the amount of atmosphere that the laser beam has to traverse, thereby reducing attenuation and beam spreading. However, this advantage comes at the cost of more difficult pointing due to the instability of the aircraft in flight.

There is no public information on the progress of the project and when it is expected to be fully tested and ready for deployment. However, it is interesting to note that recent statements concerning the A-60 laser aircraft have not made reference to an ASAT mission but have referred to a combat aircraft "capable of destroying enemy targets with a high accuracy laser."[200] Although far from conclusive, this may indicate a multi-purpose role for the aircraft.

Satellite Laser Ranging (SLR): Potential for Laser Dazzling

Russia has nine stations that are part of the International Laser Ranging Service Satellite (ILRS) network.[201] The ILRS network supports laser ranging measurements to cooperative satellites with retro-reflector arrays for scientific purposes. Although it is not their purpose, the stations could be used to dazzle optical imaging satellites (but is harmless to other types of satellites).[202] Additionally, Russia could establish a network of laser dazzling stations near sensitive sites using SLR technology. However, there is no public indication of this occurring, and SLR technology capable of this is not unique to Russia.

Space-Based Laser ASAT

During the 1970's, the USSR researched the development of a space-based high-power laser for anti-satellite missions.[203] The Soviet program resulted in the production of a test platform known as Skif-DM (or Polyus). The Skif-DM vehicle was a very large spacecraft (approximately 80,000 kg) that was to be orbited by the very large Energia space launch vehicle used to launch the Buran space shuttle.[204] The Energia launch of the Skif-DM on May 11, 1987, was a failure, attributed to an attitude control problem on the Skif-DM payload itself, and the payload fell into the Pacific Ocean.[205] The Skif-DM spacecraft was reportedly a test vehicle for a 1 megawatt carbon dioxide laser. No other launches of similar test spacecraft were attempted, and the program was likely abandoned in the turmoil of the dissolution of the USSR in 1991. This was also the final flight of the Energia SLV, which was also abandoned together with the Buran space shuttle program.[206]

---

[200] "Russia's New Combat Aircraft A-60 to be Armed With High Accuracy Laser — KRET," *TASS*, September 26, 2016, http://tass.com/defense/902173.
[201] International Laser Ranging Service web page, List of Stations; online https://ilrs.cddis.eosdis.nasa.gov/network/stations/index.html.
[202] Yousaf Butt, "Effects of Chinese Laser Ranging on Imaging Satellites," *Science and Global Security*, 17:20-35, 2009, https://www.princeton.edu/sgs/publications/sgs/archive/17-1-Butt-Effects-of-Chinese.pdf.
[203] Dwayne A. Day, and Robert G. Kennedy III, "Soviet Star Wars," *Air and Space Magazine*, January 2010, https://www.airspacemag.com/space/soviet-star-wars-8758185/?all.
[204] Ibid.
[205] "Polyus/Skif-DM," *Buran-Energia.com*, accessed March 16, 2018, http://www.buran-energia.com/polious/polious-desc.php.
[206] Dwayne A. Day, and Robert G. Kennedy III, "Soviet Star Wars," *Air and Space Magazine*, January 2010, https://www.airspacemag.com/space/soviet-star-wars-8758185/?all.

Operating a high-power space-based laser would be a very demanding technological challenge. Achieving high enough power to damage or destroy satellites would require either a large chemical laser or a large solid-state laser. The chemical laser would require a large store of feed chemicals in order to operate for more than a few seconds. Also, venting of the exhaust gases during operation would pose stability challenges for the spacecraft. A solid-state laser would require a large electrical generation capacity. If achieved with solar panels, a very large array would be required. It would not be possible to surreptitiously deploy either of these concepts in orbit.

There is no evidence that Russia has either the technological capacity or the intent to pursue a space-based laser ASAT capability at this time.

Potential Military Utility

Directed energy weapons offer similar potential military utility to electronic warfare weapons. They can be used to nullify specific military space capabilities, and often be able to do so without causing long-term damage or large amounts of space debris. In some situations, use of DEW could be seen as less escalatory than a kinetic attack on a satellite, potentially creating a way to disable military space capabilities without being considered an armed attack.

However, DEW counterspace capabilities do have significant drawbacks. DEW technologies that can do physical damage have proven difficult to perfect, and also pose operational challenges with limited fuel capacity, firing times, and range. Additionally, it can be very difficult to determine the threshold between temporary dazzling or blinding and causing long-term damage, particularly since it may depend on the internal design and protective mechanisms of the target satellite that are not externally visible. Moreover, it can be difficult for an attacker to determine whether or not a non-destructive DEW attack actually worked.

2.5 - Russian Policy and Doctrine

Russian Military Thought and Initiatives on Space and Conflict

Having observed the U.S. way of war during the past several decades, the Russian political and military leadership have come to see the military aspect of space as essential to modern warfare and winning current and future conflicts. While it is true that the Russian military sees the U.S. reliance on space-based assets as a vulnerability to be exploited, Russian thinking about conflict in space and space in conflict is much more a reflection of the evolution of modern warfare and the struggle to achieve information dominance during military operations.[207] To that end, the Russian military is aggressively pursuing capabilities to degrade or destroy adversary space-based assets as well as negate the advantage of space-based capabilities in theaters of conflict. At the same time, the Russian military is expanding its own presence in space and its ability to use space-based capabilities to enhance the performance of its forces in conflict. Given Russian views of the nature of warfare and its perceptions of the threat environment facing the Russian Federation, Russian investment in the space domain is certain to continue.

Russian Views of Space and Modern Warfare

Russian leadership and military assessments of the security aspect of space must be understood within the larger context of Russian views of modern warfare. Russian strategists see the trajectory of modern warfare being dominated by the struggle to achieve information dominance as a prerequisite to military victory.[208]

Information-driven modern technologies ranging from long-range precision strike platforms to offensive cyber capabilities are driving a Russian view of modern conflict as evolving toward non-contact warfare (*beskontaktnaia voenna*). According to this view, technological advancements enable adversaries to target and conduct offensive operations against each other's assets and critical infrastructure without entering the physical geographic theater of conflict. [209] This concept also appears in Russian military at times under different rubrics such as 6th generation warfare in the 1990s and early 2000s, and perhaps more recently as 'new type warfare.'

Space-based, information-driven military capabilities make non-contact warfare possible, through such enabling actions as queuing and guidance of long-range strike assets. And this is but one application of space-enabled information. Russian security strategists believe the struggle for information dominance begins before conflict and, once conflict has ensued, is used to dominate

---

[207] S.G. Chekinov, and S.A. Bogdanov, "Evolution of the Essence and Content of the Concept of War in the 21st Century," Voennaia mysl, no. 1 (2017), https://dlib.eastview.com/browse/doc/48113925; Daniel Coats, "Worldwide Threat Assessment of the U.S. Intelligence Community: Statement for the Record," March 6, 2018, https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1851-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community.

[208] Anton Petrov, "Future Warfare," *Moscow Defense Brief*, no. 3 (2016), accessed March 15, 2018, http://www.mdb.cast.ru/mdb/3-2016/item1/article1/.

[209] S.G. Chekinov, and S.A. Bogdanov, "Evolution of the Essence and Content of the Concept of War in the 21st Century," Voennaia mysl, no. 1 (2017), https://dlib.eastview.com/browse/doc/48113925.

an opponent's decision making by either denying the adversary's ability to utilize space-enabled information or by corrupting that information to mislead an adversary into making decisions contrary to their military objectives.[210]

Space in Conflict

The role of space in conflict is to provide the information necessary to employ one's forces and weapons and to deny that ability to one's adversary. The Russian military has invested heavily in electronic warfare, in part, to mitigate U.S. space-based capabilities.

During the late 1990's and early 2000's, Russia's GLONASS satellite system had atrophied to a mere seven satellites, not enough for effective military application. For example, in the first Chechnyan war from 1994-1996, Russian pilots and ground forces came to rely, in part, on western-based GPS navigation systems.[211]

Since 2011, Russia has maintained the minimum 24 GLONASS satellites necessary for its military applications.[212] The return of Russian space-based capabilities is increasing the capability and effectiveness of Russian forces and weapons platforms—a capability that some Russian writers suggest signals Russia's ability to conduct noncontact warfare.[213] A fully functioning GLONASS architecture benefits Russian forces in navigation, PGM employment, and command and control. For example, satellite-based course correction for some Russian PGMs decreased the impact deviation from 30 to less than 10 meters.[214] In Syria, Russian forces have used satellite-enabled weapons ranging from more accurate air-launched and dropped munitions to sea-based PGM employment.[215] Satellite navigation has also improved Russian situational awareness on the ground.[216]

Russian capabilities to deny an adversary's use of space-based information span the military spectrum from the tactical through the operational and into the strategic levels of war. At the tactical level, GPS jamming platforms such as the Zhitel, would be employed in conflict to deny western forces the use of GPS.[217] At the operational-strategic level, other systems would challenge western military forces use of satellite-based communications over large sections of the battlefield.[218] The Russian military is integrating these capabilities into all of its combat units down

---

[210] Yu Donskov, A.L. Moraresku, and V.V. Panasyuk, "On the Issue of Disorganization of Command and Control," Voennaia mysl, no. 8 (2017).
[211] Anton Lavrov, "Russia's GLONASS Satellite Constellation," *Moscow Defense Brief*, no. 4 (2017), http://www.mdb.cast.ru/mdb/4-2017/item2/article3/.
[212] Ibid.
[213] Constantine Bogdanov, "Russian Operations in Syria," *Natsional'naia oborona*, no. 12 (2017).
[214] Ibid.
[215] Dmitry Kornev, "Russian High-Precision Weapons in Syria," *Moscow Defense Brief*, no. 3 (2016), http://www.mdb.cast.ru/mdb/3-2016/item4/article1/.
[216] Anton Lavrov, "Russia's GLONASS Satellite Constellation," *Moscow Defense Brief*, no. 4 (2017), http://www.mdb.cast.ru/mdb/4-2017/item2/article3/.
[217] Roman Skomorokhov, "Станция постановки помех Р-330Ж «Житель»," accessed March 15, 2018, https://topwar.ru/98467-stanciya-postanovki-pomeh-r-330zh-zhitel.html.
[218] Dimitry Yurov, "Мат в два хода: как «Мурманск-БН» нейтрализует силы НАТО за минуты [Mate in two moves: how 'Murmansk-BN' neutralizes NATO forces in minutes]," *Tvzezda,ru*, October 18, 2016, https://tvzvezda.ru/news/forces/content/201610180741-uzd8.htm.

to the lowest level with an understanding that information warfare, to include space-based capabilities, is essential to winning in modern warfare.

Conflict in Space

There is an obvious overlap between space in conflict and conflict in space. Considerations of the military aspects of the space domain drive several concerns and initiatives from the Russian political and military leadership. First, as noted earlier, the Russian military sees the U.S. reliance on space-based capabilities as a potential vulnerability to be exploited during conflict. The Russian forces also see their own space-based capabilities as enabling more effective early warning and combat operations, especially when one considers the contrast between operations against Georgia and recent operations in Syria. However, based on an understanding of the U.S. vulnerability, the Russian military understands that its own space-based capabilities are a vulnerability that must be mitigated through both offensive means and retaining key capabilities and knowledge that is not reliant on space-based information. Finally, the Russian leadership is concerned about the possibility of space-based weapons that can target ground-based assets and critical infrastructure.

One could argue, based on public Russian statements and initiatives, such as promoting treaties against the weaponization of space, that the Russian concern over the militarization of space is in response to U.S. initiatives.[219] It is more likely, however, that Russian strategists see space as a natural domain within which competition and conflict will grow. Motivations aside, Russian military leaders and the defense industry are aggressively pursuing destructive and nondestructive ground, air, and space-based anti-satellite capabilities.[220]

Russian objectives in space, however, face significant challenges over the near term primarily from industry shortcomings.[221] The Ukraine conflict and the subsequent sanctions placed on the Russian Federation brought to light several Russian industrial and technological deficiencies in its space program such as the hardening and miniaturization of electronics.[222] Despite these challenges, Russian President Vladimir Putin recently announced a number of initiatives suggesting that Russia intends to aggressively address its shortfalls in space.[223]

---

[219] "Рогозин предупредил о необратимых последствиях размещения оружия США в космосе [Rogozin warned about the irreversible consequences of placing U.S. weapons in space]," *VPK*, March 14, 2018, https://vpk-news.ru/news/41695; Vladimir Kozin, "Pentagon Rushes Into Space," Red Star, 2017, No. 2 37," accessed March 11, 2018, https://dlib.eastview.com/search/pub/doc?art=64&id=48594676 ; B.L. Zaretsky, "Aerospace Security of Russia - VM," *Voennaia mysl*, no. 9 (2015), https://dlib.eastview.com/browse/doc/45346075.

[220] Daniel Coats, "Worldwide Threat Assessment of the U.S. Intelligence Community: Statement for the Record," March 6, 2018, https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1851-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community.

[221] Victor Mokhov, "Russian Satellites: Failure After Failure," *Moscow Defense Brief*, no. 6 (2015), http://www.mdb.cast.ru/mdb/6-2015/item3/article1/.

[222] Ivan Cheberko, "Launch of the Satellite System Arktika is Postponed Until 2018," *Defense & Security*, 2016, No. 967," accessed March 11, 2018, https://dlib.eastview.com/search/pub/doc?art=11&id=47537968.

[223] "Путин анонсировал полет российской миссии на Марс в 2019 году," accessed March 15, 2018, http://www.interfax.ru/russia/603683 ; "Путин рассказал о новых космических проектах России," accessed March 15, 2018, https://www.vesti.ru/doc.html?id=2876961

Conclusion

The views and initiatives of the Russian political and military leadership are a result of more than just the perceived vulnerability of U.S. space-enabled capabilities and operations. Russian military thinkers see modern warfare as a struggle over information dominance and net-centric operations that can often take place in domains without clear boundaries and contiguous operating areas. To meet the challenge posed by the space-aspect of modern warfare, Russia is pursuing lofty goals of incorporating electronic warfare capabilities throughout its military to both protect its own space-enabled capabilities and degrade or deny those capabilities to its adversary. In space, Russia is seeking to mitigate the superiority of U.S. space assets by fielding a number of ground, air, and space-based offensive capabilities. Although technical challenges remain, the Russian leadership has indicated that Russia will continue to seek parity with the United States in space.

3 – UNITED STATES OF AMERICA

The United States currently has the best military space capabilities in the world. During the Cold War, the United States pioneered many of the national security space applications that are in use today and remains the technology leader in nearly all categories. The U.S. military also has the most operational experience of any military in the world in integrating space capabilities into military operations, having done so in every conflict since the 1991 Persian Gulf War against Iraq.

During the Cold War, the United States, like the Soviet Union, had multiple counterspace programs, ranging from nuclear-tipped missiles to conventional DA-ASATs launched from fighter jets. Most of these programs were aimed at countering specific Soviet military space capabilities, such as the ability to use satellites to target U.S. Navy ships with anti-ship missiles. After the fall of the Soviet Union, the United States briefly considered pushing ahead and developing new counterspace systems to solidify its space superiority. However, these efforts never fully materialized due to a range of factors, including domestic budgetary and political pressure, a deliberate act of self-restraint, and the focus on counterterrorism and counterinsurgency campaigns following the 9/11 terrorist attacks.

Today, the United States fields one acknowledged counterspace system and has an electronic warfare capability, but it also has multiple other operational systems that could be used in a counterspace role. There is evidence to suggest a robust debate is underway, largely behind closed doors, on whether the United States should develop new counterspace capabilities, both to counter or deter an adversary from attacking U.S. assets in space and to deny an adversary their own space capabilities in the event of a future conflict. The impetus for this debate is renewed Russian and Chinese counterspace development, and the recent conclusion that the United States is engaged in great power competition with Russia and China.

The following sections summarize U.S. counterspace development across co-orbital, direct ascent, directed energy, and electronic warfare categories, along with a summary of U.S. policy and doctrine on counterspace.

3.1 - U.S. Co-Orbital ASAT

Assessment

The United States has conducted multiple tests of technologies for close approach and rendezvous in both LEO and GEO, along with tracking, targeting, and hit-to-kill intercept technologies that could lead to a co-orbital ASAT capability. These tests and demonstrations were conducted for other non-offensive missions, such as missile defense, on-orbit inspections, and satellite servicing, and the United States does not have an acknowledged program to develop co-orbital capabilities. However, the United States possesses the technological capability to develop a co-orbital capability in a short period of time if it chooses to.

Specifics

Although the United States has never had an officially recognized co-orbital ASAT program, it did test and develop many of the underlying technologies as part of its missile defense programs during the Cold War. Most notably, several of the technologies for space-based midcourse ballistic missile intercept developed as part of the SDI during the 1980s could have been used to intercept satellites as well.

Cold War Testing

The United States did conduct a successful on-orbit intercept during the Delta 180 experiment as part of the Strategic Missile Defense Initiative. The goal of the Delta 180 experiment was to better understand tracking, guidance, and control for a space intercept of an accelerating target.[224] The experiment involved modifying the second stage of a Delta 2 rocket (D2) to carry a sophisticated tracking system that included ladar, ultraviolet, visible, and infrared sensors. The payload consisted of a McDonnell Douglas PAS (Payload Assist System) platform combined with the warhead and seeker from a Phoenix air-to-air missile and Delta 2 rocket motors. The Delta 180 rocket was launched from the Cape Canaveral Air Force Station (CCAFS) on September 5, 1986, and the D2 and PAS were placed into a 220-km circular orbit. The PAS maneuvered to a separation distance of 200 km, and 90 minutes after launch, the D2 observed the launch of an Aries rocket from White Sands Missile Range. At 205 minutes after launch, the D2 and PAS both ignited their engines on an intercept course, colliding at a combined speed of nearly 3 km/s.[225] Sixteen pieces of orbital debris from the collision were cataloged with apogees as high as 2,300 km. However, the low altitude of the intercept resulted in all pieces reentering the atmosphere within two months.

Recent LEO RPO Activities

Since the end of the Cold War, the U.S. Air Force (USAF), National Aeronautics and Space Administration (NASA), and Defense Advanced Research Projects Agency (DARPA) have all

[224] John Dassoulas and Michael D. Griffin, "The Create of the Delta 180 Program and Its Follow-ons," *Johns Hopkins APL Technical* Digest, vol. 11, Numbers 1 and 2 (1990): p.86, http://www.jhuapl.edu/techdigest/views/pdfs/V11_1-2_1990/V11_1-2_1990_Dassoulas.pdf.
[225] "VSE (Delta-180, DM-43)," Gunter's Space Page, accessed March 22, 2018, http://space.skyrocket.de/doc_sdat/vse.htm.

conducted tests and demonstrations of close approach and rendezvous technologies in LEO. On January 29, 2003, the USAF launched the XSS-10 as a secondary payload on a Delta-2 rocket carrying a U.S. military GPS satellite. After the GPS satellite was deployed and the Delta upper stage conducted its passivization burns, the XSS-10 was released. It then conducted a pre-planned series of RPO maneuvers near the Delta upper stage, eventually closing to within 50 m (165 ft).[226] XSS-11 was launched on April 11, 2005, and according to the official fact sheet, proceeded to "successfully demonstrate rendezvous and proximity operations with the pended rocket body [that placed it in orbit]."[227] The fact sheet also stated that over the following 12 to 18 months, the spacecraft "conduct[ed] rendezvous and proximity maneuvers with several US-owned, dead or inactive resident space objects near its orbit." However, it is impossible to verify whether or not these activities occurred, and whether or not XSS-11 visited any non-U.S. space objects, because the U.S. military did not publish any positional information for the XSS-11 while on orbit.

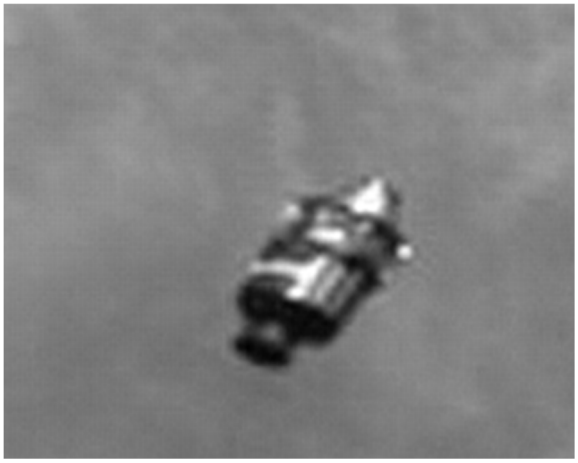

Figure 9 - Minotaur upper stage
Image taken by XSS-11 from a distance of approximately 500 m.
Image credit: AFRL.[228]

On April 15, 2005, NASA launched the DART satellite to conduct an autonomous rendezvous experiment with a U.S. Navy communications satellite, the MUBLCOM satellite. DART ended up "bumping" into MUBLCOM during the test, and although both satellites were apparently unharmed, the public version of NASA's mishap report lacks details as to why the collision happened.[229]

---

[226] Thomas M. Davis and David Melanson, "XSS-10 Micro-Satellite Flight Demonstration," Paper No. GT-SSEC.D.3: p.7. https://smartech.gatech.edu/bitstream/handle/1853/8036/SSEC_SD3_doc.pdf;jsessionid=906BB52FE69F848048883B704DB20F07.smart2?sequence=2.
[227] "XSS-11 Micro Satellite," Fact Sheet: Air Force Research Laboratory, Space Vehicles Directorate, current as of September 2011, accessed March 22, 2018, p.1, http://www.kirtland.af.mil/Portals/52/documents/AFD-111103-035.pdf?ver=2016-06-28-110256-797.
[228] "XSS-11 Micro Satellite," p.2
[229] "Overview of the DART Mishap Investigation Results," NASA, accessed March 22, 2018, http://www.nasa.gov/pdf/148072main_DART_mishap_overview.pdf.

DARPA also conducted a demonstration of close approach and rendezvous technology in the context of satellite servicing with its Orbital Express mission. Orbital Express consisted of two spacecraft, the ASTRO servicing vehicle and the NEXTSat client vehicle. On March 8, 2007, the two spacecraft were launched from CCAFS on an Atlas V rocket and placed into a roughly 500 km circular orbit. After checkout, the ASTRO demonstrated the ability to autonomously transfer fluid to NEXTSat and use a robotic arm to swap out components. The two spacecraft then separated, and spent few months demonstrating multiple rendezvous and capture scenarios, including the first-ever use of a robotic arm to autonomously capture another space object.[230] The two spacecraft were deactivated in July 2007.[231]

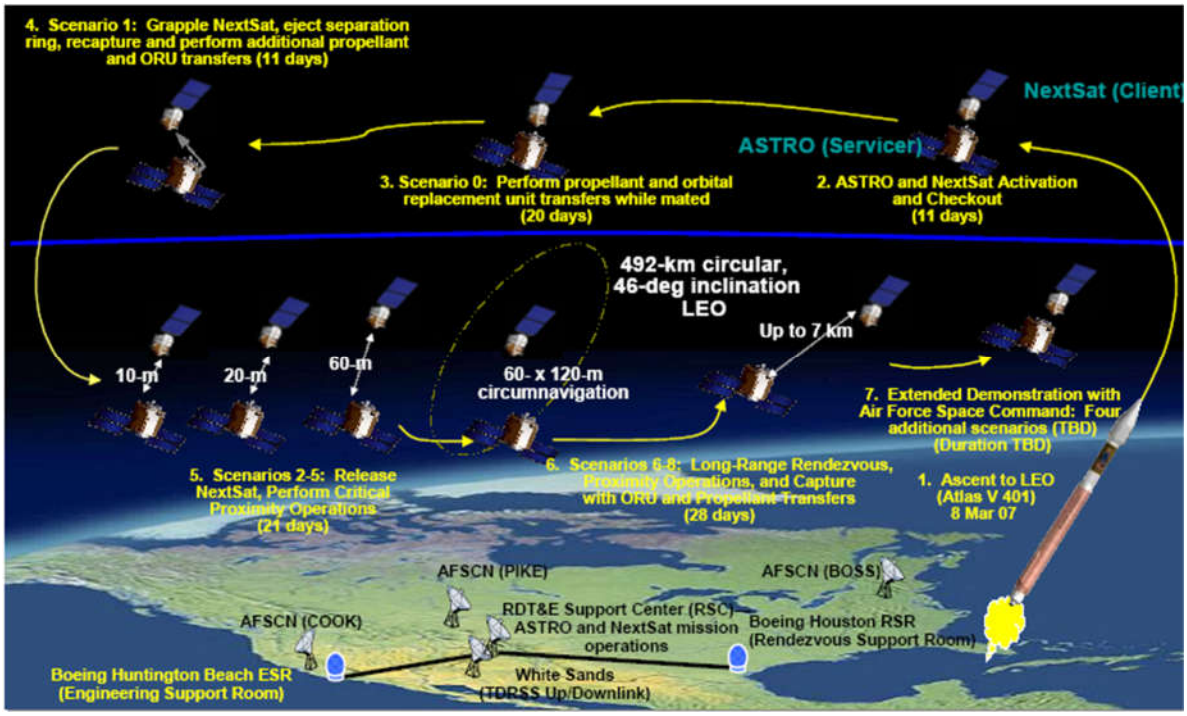

Figure 10 - Orbital Express mission plan
Image credit: Boeing.[232]

Recent GEO RPO Activities

The United States has also conducted multiple close approach and proximity operations in GEO. The earliest known example is a satellite reportedly called Prowler. Based on publicly-available data, satellite observer Ted Molczan concluded that Prowler was secretly launched from a Space

[230] "Orbital Express – Mission Updates," Boeing, Defense, Space & Security PhantomWorks, accessed March 22, 2018, https://web.archive.org/web/20121017163534/http://www.boeing.com/bds/phantom_works/orbital/updates.html.
[231] Stephen Clark, "In-space Satellite Servicing Tests Come to an End," *SpaceFlight Now*, July 4, 2007, http://spaceflightnow.com/news/n0707/04orbitalexpress/.
[232] "Orbital Express: Testing On-Orbit Servicing," *Defense Industry Daily*, April 19, 2007, https://www.defenseindustrydaily.com/orbital-express-is-that-a-new-battery-or-are-you-just-glad-to-see-me-03220/.

Shuttle mission in 1990,[233] and matched the description given in a 2004 NBC news article about a classified U.S. government satellite program that had run afoul of Congress.[234] The satellite had reportedly maneuvered close to multiple Russian geosynchronous orbit (GSO) satellites to collect intelligence on their characteristics and capabilities, and utilized stealth technologies to remain undetected by Russian optical space surveillance systems. To this day, the United States has never officially acknowledged the existence of Prowler and lists it as an extra rocket body from the Shuttle launch in its public satellite catalog.

While Prowler is thought to have been decommissioned in around 1998, it was followed by programs designed for similar missions. In 2006, the USAF launched two small satellites into GSO, officially designated as Micro-satellite Technology Experiment (MiTEx), with the official mission to identify, integrate, test, and evaluate small satellite technologies to support and enhance future U.S. space missions.[235] Observers speculated that the MiTEx satellites would be conducting RPO in GSO.[236] In 2009, news reports revealed that they had been used to conduct "flybys" of the U.S. early warning satellite DSP 23, which had mysteriously failed on orbit shortly after launch.[237] Observations from hobbyists noted that the two MiTEx satellite maneuvered from their parking slots in GSO to drift towards the location of DSP 23, passing it around December 23, 2009, and January 1, 2010.

In recent years, the USAF appears to have applied the lessons it learned with Prowler and MiTEx to an operational program known as the Geostationary Space Situational Awareness Program (GSSAP). GSSAP uses two pairs of small satellites deployed in near-GEO orbits, with altitudes slightly above and below the GSO belt, which allow them to drift east and west and provide close inspections of objects in the GEO region.[238] The official USAF fact sheet states that the GSSAP satellites are able to conduct RPO of "resident space objects of interest."[239] The first pair of GSSAP satellites were launched on July 28, 2014, and the second pair on August 19, 2016, both times on a Delta 4 rocket from CCAFS. Very limited public information is known about the on-orbit activities of the four GSSAP satellites, as the USAF does not disclose information on their orbits. A third pair is slated for launch in 2020.[240]

---

[233] Ted Molczan, "Unknown GEO Object 2000-653A/90007 Identified as Prowler," January 21, 2011, p. 12, http://satobs.org/seesat_ref/STS_38/Unknown_GEO_Object_2000-653A_-_90007_Identified_as_Prowler.pdf.
[234] Robert Windrem, "What is America's Top-Secret Spy Program? Experts Think Democrats Objected to Satellite Weapon," *NBC News,* December 9, 2004, http://www.nbcnews.com/id/6687654/ns/us_news-security/t/what-americas-top-secret-spy-program/ .
[235] Justin Ray, "Experimental Military Microsatellites Reach Orbit," *Spaceflight Now*, June 22, 2006, https://www.space.com/2529-experimental-military-microsatellites-reach-orbit.html.
[236] Ryan Caron, "Mysterious Microsatellites in GEO: is MiTEx a Possible Anti-Satellite Capability Demonstration?" *TheSpaceReview.com,* July 31, 2006, http://www.thespacereview.com/article/670/1.
[237] Brian Weeden, "The Ongoing Saga of DSP Flight 23," *TheSpaceReview.com,* January 19, 2009, p.1, http://www.thespacereview.com/article/1290/1.
[238] Amy Butler, "USAF Reveals Sats to Offer Unprecedented Space Intel," *Aviation Week & Space Technology,* March 3, 2004, http://aviationweek.com/awin/usaf-reveals-sats-offer-unprecedented-space-intel.
[239] "Geosynchronous Space Situational Awareness Program," USAF Fact Sheet, March 22, 2017, http://www.afspc.af.mil/About-Us/Fact-Sheets/Article/730802/geosynchronous-space-situational-awareness-program-gssap/.
[240] "GSSAP 1, 2, 3, 4, 5, 6," Gunter's Space Page, accessed March 22, 2018, http://space.skyrocket.de/doc_sdat/gssap-1.htm.

On September 18, 2015, General John E. Hyten, then Commander of U.S. Air Force Space Command, remarked at a public forum that the two GSSAP satellites had been "pressed into early service" to provide information to an un-named customer.[241] According to General Hyten, the two satellites provided what he deemed "eye-watering" pictures of one or more objects in GSO.

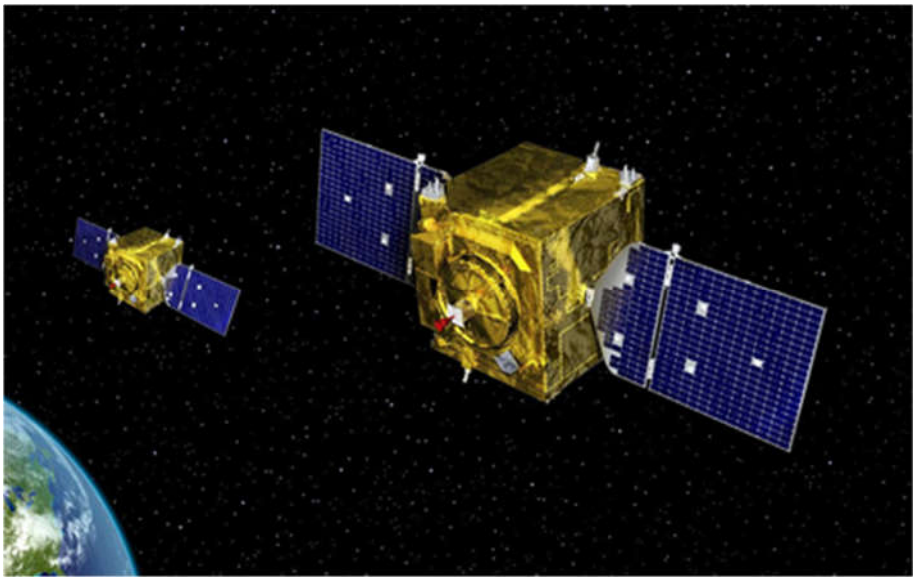

Figure 11 - GSSAP satellites
Artist's depiction.
Image credit: U.S. Air Force.[242]

The USAF also announced that the launch of the first two GSSAP satellites included a satellite from another RPO program, the Automated Navigation and Guidance Experiment for Local Space (ANGELS) Program.[243] The goal of ANGELS was to provide a clearer picture of the local area around important U.S. national security satellites in GSO. The first ANGELS satellite stayed attached to the Delta 4 upper stage while it placed the first GSSAP pair into GSO and conducted a disposal maneuver to place it a few hundred km above GSO. At that point, ANGELS detached from the upper stage and conduct a series of RPO maneuvers to close within a few kilometers.[244] No independent verification of these activities is publicly available, and the USAF has not disclosed orbital information for either ANGELS or the Delta 4 upper stage. ANGELS was decommissioned in November 2017.[245]

---

[241] Mike Gruss, "Space Surveillance Sats Pressed Into Early Service," *Space News*, September 18, 2015, http://spacenews.com/space-surveillance-sats-pressed-into-early-service/.
[242] "Geosynchronous Space Situational Awareness Program," USAF Fact Sheet.
[243] Stephen Clark, "Air Force General Reveals New Space Surveillance Program," *SpaceFlight Now,* February 25, 2014, http://spaceflightnow.com/news/n1402/25gssap/.
[244] "Fact Sheet: Automated Navigation and Guidance Experiment for Local Space," Air Force Research Laboratory, current as of July 2014, accessed March 22, 2018, p. 1, http://www.kirtland.af.mil/Portals/52/documents/AFD-131204-039.pdf?ver=2016-06-28-105617-297.
[245] Arielle Vasquez, "3rd SES Bids Farewell to ANGELS Satellite," 50th Space Wing Public Affairs, November 21, 2017, http://www.patrick.af.mil/News/Article-Display/Article/1378964/3rd-ses-bids-farewell-to-angels-satellite/.

Potential Military Utility

The most likely military utility of the capabilities demonstrated by the DART, XSS-10, XSS-11, Orbital Express, Prowler, MiTEx, GSSAP, and ANGELS satellites is for on-orbit SSA and close-up inspections. What little is known of their operational pattern is consistent with slow, methodical, and careful approaches to rendezvous with other space objects in similar orbits. The satellites they are known to have approached were in similar orbits and based on the publicly available data they did not make huge changes to rendezvous with satellites in significantly different orbits. This behavior is similar to several international RPO missions to test and demonstrate satellite inspection and servicing capabilities, in particular the Chinese SJ-12, SJ-15, SJ-17 satellites and the Russian Cosmos 2499, Cosmos 2501, and Cosmos 2521 satellites.

The Delta 180 mission did include explicit testing of offensive capabilities, and in particular the ability to physically collide with another satellite to damage or destroy it. However, the deliberate maneuvering to create a conjunction with the target satellite would be detectable with existing processes already in place to detect accidental close approaches. Warning time of such a close approach would likely be at least hours (for LEO) or days (for GEO), unless the attacking satellite was already in a very similar orbit.

3.2 - U.S. Direct-Ascent ASAT

Assessment

While the United States does not have an operational, acknowledged DA-ASAT capability, it does have operational midcourse missile defense interceptors that have been demonstrated in an ASAT role against low LEO satellites. The United States has developed dedicated DA-ASATs in the past, both conventional and nuclear-tipped, and likely possesses the ability to do so in the near future should it choose so.

Specifics

ASM-135 Air-Launched DA-ASAT

The ASM-135 was an air-launched missile developed in response to the Soviet Union's successful demonstration of a co-orbital ASAT capability and intended to fulfill the DA-ASAT role without requiring the use of nuclear weapons.[246] The missile, produced in 1984, was designed to be launched from a modified F-15A in a supersonic zoom climb and intercept targets in LEO.[247] Five flight tests occurred,[248] the most famous of which was an intercept test on September 13, 1985, in which the Solwind P78-1 satellite was destroyed at an altitude of 555 km, marking the only time that a U.S. missile destroyed a satellite prior to 2007.[249]

The ASM-135 had an estimated operational range of 648 km, flight ceiling of 563 km, and speed of over 24,000 km/h.[250] The missile incorporated an infrared homing seeker guidance system, and three rocket stages: a modified Boeing AGM-69 SRAM with a Lockheed LPC-415 solid propellant two pulse rocket engine, an LTV Aerospace Altair 3 using a Thiokol FW-4S solid propellant rocket engine and equipped with hydrazine-fueled thrusters for finer maneuvering to target, and an LTV-produced interceptor named the Miniature Homing Vehicle (MHV) equipped with 63 small rocket motors for fine trajectory adjustments and attitude control.[251]

---

[246] Andreas Parsch, "Vought ASM-135 ASAT," *Directory of U.S. Military Rockets and Missiles*, updated December 29, 2004, http://www.designation-systems.net/dusrm/m-135.html.

[247] Ibid.

[248] The four other tests include: a successful missile test without the MHV on January 21, 1984; a failed missile test directing MHV at a star on November 13, 1984; and two successful flight tests directing MHV at a star on August 22, 1986 and September 29, 1986. Gregory Karambelas and Sven Grahn, "The F-15 ASAT Story," http://www.svengrahn.pp.se/histind/ASAT/F15ASAT.html; Raymond Puffer, "The Death of a Satellite," *Air Force Flight Test Center History Office*, archived from web in 2003, https://web.archive.org/web/20031218130538/http://www.edwards.af.mil/moments/docs_html/85-09-13.html.

[249] "Vought ASM-135A Anti-Satellite Missile," *National Museum of the U.S. Air Force*, March 14, 2016, http://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/198034/asm-135-asat/.

[250] Parsch, "Vought ASM-135 ASAT."

[251] "ASAT Overview," *Vought Heritage Website*, archived from web in 2007, https://web.archive.org/web/20070131173354/http://www.vought.com/heritage/products/html/asat.html; "Altair 3," *Encyclopedia Astronautica*, archived from web in 2008, https://web.archive.org/web/20080202163409/http://www.astronautix.com/stages/altair3.htm.

The U.S. Air Force had planned to deploy an operational force of 112 ASM-135 missiles, to be deployed aboard 20 modified F-15s.[252] 15 ASM-135 missiles were ultimately produced, five of which were used in flight tests, and a number of airframes were modified to support its use. In 1988, due to a mix of budgetary, technical, and political concerns, the Reagan Administration mothballed the program, though the expertise and technical capability likely remain intact.

Midcourse Missile Defense Systems as Anti-Satellite Weapons

Because midcourse missile defense systems are intended to destroy long-range ballistic missile warheads, which travel at speeds and altitudes comparable to those of satellites, such defense systems also have inherent ASAT capabilities. In many ways, attacking satellites is an easier task than defending against ballistic missiles. Satellites travel in repeated, predictable orbits and observations of the satellite can be used to predict its future position. While the launch of a ballistic missile may occur with little or no advanced notice, an anti-satellite attack could be planned in advance to be under the most convenient conditions, and the attacker may be able to try multiple times if the first try fails.

The United States currently has two operational midcourse missile defense systems that have latent DA-ASAT capabilities: the ground-based interceptors (GBIs), part of the Ground-based Midcourse System (GMD), and the ship-based Standard Missile 3 (SM-3) interceptors, part of the Aegis system. Of the two, only the SM-3 has been demonstrated in a DA-ASAT role. In 2008, the U.S. Operation Burnt Frost used a SM-3 Block IA interceptor fired from an Aegis Cruiser to destroy an ailing U.S. reconnaissance satellite at an altitude of 240 km.[253] Three SM-3 missiles had a "one-time software modification" to enable them to intercept the satellites, but it is impossible for an adversary to verify whether any additional SM-3 interceptors have been modified for ASAT capability.

The GBIs have the most potential capability in a DA-ASAT role. Forty-four GBIs are currently deployed at bases in Fort Greely, Alaska, and Vandenberg Air Force Base, California.[254] The planned burnout speed of the GBIs is reported to be 7 to 8 km/s.[255] A missile with this burnout speed could lift the exoatmospheric kill vehicle (EKV) to a height of roughly 6,000 km. This puts it in reach of all satellites in low-earth orbit, and possibly some satellites in highly elliptical orbits with perigees that dip down into these altitudes. The GBI could not reach satellites in much higher MEO or GEO.

---

[252] Parsch, "Vought ASM-135 ASAT."
[253] "Navy Missile Hits Dying Spy Satellite, Says Pentagon," *CNN,* February 21, 2008, http://www.cnn.com/2008/TECH/space/02/20/satellite.shootdown/.
[254] "Ground-Based Midcourse Defense," Missile Defense Advocacy Alliance, December 1, 2017, http://missiledefenseadvocacy.org/missile-defense-systems-2/missile-defense-systems/u-s-deployed-intercept-systems/ground-based-midcourse-defense/.
[255] Laura Grego, George N. Lewis, David Wright, "Shielded from Oversight: The Disastrous US Approach to Strategic Missile Defense; Appendix 6: The Ground-Based Interceptor and Kill Vehicle," Union of Concerned Scientists, July 2016: p. 1, https://www.ucsusa.org/sites/default/files/attach/2016/07/Shielded-from-Oversight-appendix-6.pdf.

The EKV will be guided toward the predicted position of the satellite by ground-based radar data. From there, the sensors on the EKV use light in two infrared bands, designed to detect light emitted by room-temperature ICBM-launched warheads or sunlight reflected off them in their journey through the vacuum of space. Their ability to home on any given satellite depends on the satellite's particular properties including its operating temperature, its surface properties and whether it is in sunlight. Note that while low-Earth orbiting satellites may enter and exit the Earth's shadow repeatedly during a day, an attacker has the advantage of being able to choose the most advantageous time of attack.

The current SM-3 interceptors are less capable as DA-ASATs than the current GBIs but do have other advantages. The current Aegis interceptors SM-3 IA/ IB can reach only the relatively few satellites in orbits with perigees at or below 600 km altitude.[256] However, the SM-3 Block IIA interceptors, currently under joint development with Japan, are intended to defend larger areas against more capable threats; even using a conservative estimate of the burnout speed for such a missile (4.5 km/s), it would be able to reach the vast majority of LEO satellites as shown in Table 3-1. Interceptors with burnout speeds at the high range of estimates for the SM-3 IIA (5.5 km/s) would be able to reach any satellite in LEO.

Table 3-1 - Maxmimum altitude reachable by SM-3 variants[257]

Sm-3 Variant	Burnout Velocity (km/s)	Maximum Reachable Altitude (km)
Block 1A	3.0	600
Block IIA (lower range)	4.5	1,450
Block IIB (upper range)	5.5	2,350

The SM-3 interceptors are meant to be flexible and address emerging ballistic missile threats from the Middle East and East Asia over the coming decade. They exist not only on U.S. Navy ships that can be redeployed around the world, but also are being deployed at land-based "Aegis Ashore" sites. The initial land-based Aegis Ashore site in Romania is in operation,[258] and future sites are being developed in Poland and Japan.[259] The number of ballistic missile defense (BMD)-capable Aegis ships is expected to reach 77 by 2040,[260] which could mean the number of ASAT-capable interceptors they hold would be in the hundreds.

[256] Laura Grego, "The Anti-Satellite Capability of the Phased Adaptive Approach Missile Defense System," *Federation of American Scientists,* Winter 2011: p. 3, https://fas.org/pubs/pir/2011winter/2011Winter-Anti-Satellite.pdf.
[257] Ibid.
[258] Sam LaGrone, "Aegis Ashore Site in Romania Declared Operational," *USNI News,* May 12, 2016, https://news.usni.org/2016/05/12/aegis-ashore-site-in-romania-declared-operational.
[259] Mari Yamaguchi, "Japan to Buy Aegis Ashore Missile Defense Systems," *Associated Press,* December 19, 2017, https://www.defensenews.com/land/2017/12/19/japan-to-buy-aegis-ashore-missile-defense-systems/.
[260] "How Many Aegis BMD ships in 2040?" MostlyMissileDefense.com, December 13, 2015, https://mostlymissiledefense.com/2015/12/13/how-many-aegis-bmd-ships-in-2040-december-13-2015/.

Potential Military Utility

The SM-3 and GBI interceptors represent a potentially large and flexible DA-ASAT capability that could be used against adversary military satellites in LEO in a future conflict. Of particular interest is China's rapidly-developing space-based reconnaissance capabilities to target anti-ship ballistic missiles against U.S. ships.[261] These Chinese satellites pose a similar threat to one posed by Soviet satellites during the Cold War, against which the United States decided to develop a DA-ASAT capability.[262]

As the United States continues to build out its Aegis, GMD, and Aegis Ashore missile defense architecture, it could theoretically hold at risk a significant portion of either China's or Russia's low earth orbiting satellites, particularly if the number of Block II interceptors is increased or it is considered in concert with GMD. The Aegis ships could be positioned optimally to stage a "sweep" attack on a set of satellites nearly at once, rather than a sequential set of attacks as satellites moved into range of fixed interceptor sites. This positioning flexibility also means that the SM-3 missiles would not have to expend much of their thrust going cross-range and could retain the ability to reach the highest LEO satellites. The more powerful GMD interceptors also could use some of their fuel to reach out laterally over thousands of kilometers, allowing them to hit satellites in orbits that do not pass directly over the GMD missile fields in Alaska and California.

[261] S. Chandrashekar and Soma Perumal, "China's Constellation of Yaogan Satellites and the Anti-Ship Ballistic Missile: October 2015 Update," National Institute of Advanced Studies, October 2015: p. 10, http://isssp.in/wp-content/uploads/2015/10/Chinese-Yaogan-Satellite-Constellation-and-ASBM-Oct-2015-Update.pdf.
[262] Robert L. Smith, "Final Report of the Ad Hoc NSC Space Panel—Part II: U.S. Anti-Satellite Capabilities," National Security Council, November 3, 1976: p. 1.

3.3 - U.S. Electronic Warfare

Assessment

The United States has EW operational counterspace systems, the Counter Communications System (CCS), which can be deployed globally to provide uplink jamming capability against geostationary communications satellites.

The United States likely has the capability to jam Global Navigation Satellite System (GNSS) receivers (GPS, GLONASS, Beidou) within a local area of operation to prevent their effective use by adversaries. In addition to interfering with adversarial use of satellite navigation, the Navigation Warfare (NAVWAR) program seeks to assure the availability of GPS services for U.S. military units in operations. The effectiveness of measures to counter adversarial GPS jamming and spoofing operations is not known.

Specifics

Counter Communications System (CCS)

The Counter Communications System (CCS) program was initiated in 2003 as part of a broader counterspace capability development program. Very little information is publicly available on the CCS system or its capabilities, apart from budget documents and occasional press items. A February 2003 budget planning document describes the CCS mission. [263]

> This effort supports concept exploration and follow-on system development of a mobile/transportable counter satellite communications system and associated command and control. It includes system hardware design and development, software design and integration, testing and procurement of a capability to provide jamming of satellite communications signals in response to USSTRATCOM requirements.

The lack of public information is not surprising since the CCS is an electronic warfare (EW) system for jamming communication satellites. All EW capabilities are considered to be very sensitive and are conducted exclusively in the classified domain.

Successive annual budget planning documents have continued to provide a generic description of the CCS. In the most recently available document (2017), the description has evolved somewhat offering more insight on the role of the CCS. [264]

---

[263] "RDT&E Budget Item Justification Sheet (R-2 Exhibit), PE Number: 0604421F, PE Title: Counterspace Systems," Air Force, February 2003: p. 883, http://www.dtic.mil/descriptivesum/Y2004/AirForce/stamped/0604421F.pdf.

[264] Exhibit R-2, RDT&E Budget Item Justification: FY 2018 Air Force, Vol. 2, Program Element: PE 1206421F / Counterspace Systems, project 65A001 / Counter Satellite Communications System, May 2017: p. 699, http://www.saffm.hq.af.mil/Portals/84/documents/Air%20Force%20Research,%20Development,%20Test%20and%20Evaluation%20Vol-II%20FY18.pdf?ver=2017-05-23-160041-060.

> CCS provides expeditionary, deployable, reversible offensive space control (OCS) effects applicable across the full spectrum of conflict. It prevents adversary SATCOM in AOR including C2, Early Warning and Propaganda, and hosts Rapid Reaction Capabilities in response to Urgent Needs. This program effort includes architecture engineering, system hardware design and development, software design and integration, and testing and demonstration of capabilities to provide disruption of satellite communications signals.

There is no public information on any technical characteristic of the CCS, such as frequency ranges, power levels and waveforms. However, it is reasonable to conclude that CCS can likely jam most of the major commercial frequencies (particularly C and Ku) and the most common military frequencies (X-band), with a possible capability in the increasingly popular Ka band. Also, it is likely that the CCS is targeted mainly at geostationary communications satellites (COMSATs), given that they are currently the primary source of satellite communications.

The CCS is operated and maintained by units of the 21st Space Wing located at Peterson AFB, Colorado. The CCS units can be deployed globally to conduct mobile and transportable space superiority operations in support of global and theatre campaigns.[265]

The first two CCS units were reportedly delivered in 2004.[266] The initial systems are known as Block 10 systems. In 2012, Harris Corp, Space and Intelligence Systems, was contracted to upgrade the five existing CCS Block 10 systems to the Block 10.1 configuration.[267] In 2016, Harris again was awarded a contract to upgrade the Block 10.1 systems to the Block 20 configuration and deliver additional Block 20 systems. [268]

The total number of CCS units is not publicly known, but there are at least 13 units, since in March 2017, Harris was awarded a contract to provide Block 10.2 upgrades for 13 existing antennas across the CCS.[269]

The CCS continues to be well funded with activities including upgrades to existing systems as well as procurement of new units. The approximate funding of the program can be deduced from a series of unclassified budget planning documents available on the Defense Technical Information Center's website.[270] From 2004 to 2017, approximately $222 million has been spent on the CCS

[265] "76th Space Control Squadron Fact Sheet," Peterson AFB web site, August 16, 2012, http://www.peterson.af.mil/About/Fact-Sheets/Display/Article/326218/76th-space-control-squadron/.
[266] Jeffrey Lewis, "Counter Satellite Communications System Deployed," *ArmsControlWonk.com,* October 2, 2004, https://www.armscontrolwonk.com/archive/200025/counter-satellite-communications-system-deployed/.
[267] George I. Seffers, "Harris to Upgrade Counter Communication Systems," *Signal*, November 13, 2002, https://www.afcea.org/content/harris-upgrade-counter-communication-systems.
[268] "Harris Awarded Counter Communication System Contract," *Signal,* November 4, 2016, https://www.afcea.org/content/Blog-harris-awarded-counter-communication-system-contract.
[269] "U.S. Air Force Modifies Counter Communication System Contract," *Signal,* March 13, 2017, https://www.afcea.org/content/Blog-us-air-force-modifies-counter-communication-system-contract
[270] http://www.dtic.mil/dtic/.

program. The projected spending for the next four years (2018-2021) totals an additional $66 million.

There is no public information on theater deployments, if any, by the CCS, or the use of the system in operations, again if any. However, it is clear from the funding allocations that the CCS is a high priority program and likely offers the U.S. military a very effective SATCOM jamming capability. That CCS system continues to be evolved, presumably with increasing sophistication and capability.

NAVWAR

The United States DoD relies heavily on PNT capabilities, which are primarily provided by the GPS satellites. Over the last two decades, the U.S. military has put significant effort into incorporating GPS capabilities into a wide array of weapons systems and operational practices. Along with the enormous potential of enhancing military operations, satellite navigation systems also introduce a potential vulnerability since their precise navigation signals are also prone to interference by an adversary. In the mid-1990s, the U.S. military launched a formal effort called Navigation Warfare (NAVWAR) as part of the compromise to turn off Selective Availability for GPS. Over time, NAVWAR became a broader effort to develop a strategy for how the U.S. military could conduct both defensive and offensive operations to protect U.S. use of PNT capabilities while also interdicting or preventing adversary use of PNT capabilities. [271]

The Joint Navigation Warfare Center (JNWC) was established by Deputy Secretary of Defense Memorandum on November 17, 2004 and assigned to USSTRATCOM/JFCC SPACE in 2007. JNWC is a staff element that directly supports warfighters as the Joint Subject Matter Expert to integrate/coordinate NAVWAR across the full range of military operations for all domains, every phase of war, and the six joint warfighting functions. The JNWC's mission is "To enable Positioning, Navigation, and Timing (PNT) Superiority by providing operational NAVWAR support and by creating and maintaining NAVWAR knowledge for the Department of Defense, Interagency Partners, and the Coalition." [272]

Being an electronic warfare domain, most of the U.S. NAVWAR capabilities and activities are classified, and hence there is little publicly-available information. However, the U.S. DoD likely devotes significant resources to this domain, since space-based PNT (specifically GPS) is crucial to most military operations.

The NAVWAR defensive measures seek to prevent adversarial electronic countermeasures from interfering with the operational use of GPS in two fundamental ways. The U.S. military is developing a new military signal, called M-code, which is much more secure than the universally available civil GPS code. New generations of GPS satellites, starting with GPS III that is due to

[271] *Joint Publication 3-13.1, Electronic Warfare*, February 8, 2012, prepared under the direction of the Chairman of the Joint Chiefs of Staff (CJCS), https://info.publicintelligence.net/JCS-EW.pdf.
[272] "Joint Navigation Warfare Center (JNWC) Fact Sheet," U.S. Strategic Command, October 17, 2016, http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/976408/joint-navigation-warfare-center-jnwc/.

be launched in late 2018, will be able to broadcast M-code. The U.S. military is also developing new generations of receivers that can utilize M-code and incorporate improved anti-jam and anti-spoofing technology. The effectiveness of these measures, against a sophisticated adversary, is not known.[273]

There is no public information on the U.S. military technical capabilities for offensively jamming or spoofing adversary PNT capabilities. Nonetheless, it likely that the United States has very effective capabilities for jamming and spoofing of GNSS receivers, to include GPS, GLONASS, and Beidou. This assessment is based on the consistent high priority placed on the NAVWAR effort, the success of U.S EW systems in other domains of warfare, and the technical sophistication of the U.S. industry in this field. The most likely way this would be accomplish is by using downlink jamming to interfere with or spoof GNSS signals in a specific geographic area. [274]

Potential Military Utility

The Counter Communications System is likely very effective in denying potential adversaries of geostationary satellite communications capabilities. With COMSATs being used for an increasingly large and diverse set of critical military communications purposes (i.e. command & control, relay of intelligence and operational data, control of UAVs, etc.) the employment of CCS in theatre would likely be very effective at hampering an opponent's operations. The specific impact would depend in the circumstances of the situation.

NAVWAR, both defensive and offensive components, are essential to military operations due to the dependency on navigation services. The ability to employ precision navigation services while simultaneously denying the same to an adversary would confer a tremendous advantage in a time of conflict.

[273] Sally Cole, "Securing military GPS from spoofing and jamming vulnerabilities," *Military Embedded Systems*, November 30, 2015, http://mil-embedded.com/articles/securing-military-gps-spoofing-jamming-vulnerabilities/.
[274] Daniel Cebul, "DoD jams GPS in western states for joint exercise", *C4ISR Net*, January 26, 2018, https://www.c4isrnet.com/special-reports/pnt/2018/01/26/dod-jams-gps-in-western-states-for-joint-exercise/.

3.4 - U.S. Policy and Doctrine

National Space Policy on Counterspace

The United States has had established doctrine and policy on counterspace capabilities for several decades, although not always publicly expressed. Most recent U.S. presidential administrations have directed or authorized research and development of counterspace capabilities, and in some cases greenlit testing or operational deployment of counterspace systems. These capabilities have typically been limited in scope, and designed to counter a specific military threat, rather than be used as a broad coercive or deterrent threat.

For example, a series of policy memos in the mid-1970s recommended the development of a limited offensive counterspace capability to destroy a limited number of militarily-important Soviet space systems in a crisis situation or war.[275] The goal was to not to deter the Soviets from attacking U.S. space capabilities, but rather create the capability to reduce the Soviet ability to use space against the United States in a conflict, while limiting escalation against U.S. satellites to those in low Earth orbit. The memos specifically highlighted the use of Soviet space systems for targeting long-range anti-ship missiles against U.S. naval forces as the most critical capability to counter. The memos culminated in presidential decision directives by the Ford and Carter Administrations to develop a limited ASAT capability, along with complementary space arms control initiatives.[276] The ASAT capability eventually became the ASM-135 missile launched from an F-15 fighter aircraft.

More recent U.S. presidential decision directives are still classified, but there is evidence to suggest there is at least still some policy support for limited offensive counterspace capabilities. For example, the most recent national space policy, issued by the Obama Administration in 2010, states that the United States "will employ a variety of measures to help assure the use of space for all responsible parties, and, consistent with the inherent right of self-defense, deter others from interference and attack, defend our space systems and contribute to the defense of allied space systems, and, if deterrence fails, defeat efforts to attack them." To that end, the 2010 policy directs the Secretary of Defense shall "develop capabilities, plans, and options to deter, defend against, and, if necessary, defeat efforts to interfere with or attack U.S. or allied space systems," and "develop capabilities, plans, and options to deter, defend against, and, if necessary, defeat efforts to interfere with or attack U.S. or allied space systems." [277]

---

[275] Brent Scowcroft, "Follow-up on Satellite Vulnerability," memo to President Gerald Ford, March 15, 1976; Brent Scowcroft, "Soviet Anti-Satellite Capability," memo to President Gerald Ford, April 26, 1976.
[276] *National Security Decision Memorandum-345,* January 18, 1977; *Presidential Directive/NSC-37,* May 11, 1978.
[277] *National Space Policy of the United States of America,* June 28, 2010: p. 14, https://www.nasa.gov/sites/default/files/national_space_policy_6-28-10.pdf.

U.S. Military Doctrine on Counterspace

The link between these policy statements and offensive counterspace capabilities can be found in the official U.S. military doctrines on space operations. Two different doctrines exist on space operations: an Air Force doctrine developed by United States Air Force Space Command[278]; and a joint doctrine developed by United States Strategic Command[279]. The most recent publicly-available versions of these doctrines are June 2012 and May 2013, respectively.

Under current doctrine, the U.S. military considers space control to be a separate mission area of space operations. Space control consists of defensive space control (DSC) and offensive space control (OSC), both of which are supported by SSA. DSC consists of active and passive actions to protect friendly space-related capabilities from enemy attack or interference by protecting, preserving, recovering, and reconstituting friendly space-related capabilities before, during, and after an attack by an adversary. OSC consists of offensive operations to prevent an adversary's hostile use of U.S./third-party space capabilities or negate an adversary's space capabilities. Prevention can occur through diplomatic, informational, military, and economic measures, and negation can occur through active offensive and defense measures for deception, disruption, denial, degradation, or destruction. Ground and space-based SSA capabilities are used to find, fix, track, and target adversary space system, and assess the effects of OSC operations. OSC actions may target space nodes, terrestrial nodes, and/or communications links. To the greatest extent practicable, U.S. forces are to use OSC systems and methods which minimize risk to friendly forces, civilians, and civilian property.

Recent Policy Shifts

Since 2014, U.S. policymakers have placed increased focus on space security, and have increasingly talked publicly about preparing for a potential "war in space" and about space being a "warfighting domain". Between May and August 2014, the Department of Defense convened a Space Strategic Portfolio Review (SPR)[280], which concluded there was a need to identify threats in space, be able to withstand aggressive counterspace programs, and counter adversary space capabilities.[281] Following the SPR, senior military leadership began to talk publicly about the inevitability of conflict on earth extending to space and the need for the military to prepare to

[278] "Space Control," *Annex 3-14 Space Operations,* last updated June 19, 2012, http://www.doctrine.af.mil/Portals/61/documents/Annex_3-14/3-14-D33-SPACE-OPS-Space-Control.pdf?ver=2017-09-19-154552-817.
[279] *Joint Publication 3-14: Space Operations,* May 29, 2013, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14.pdf.
[280] Dyke Weatherington, testimony before the House Committee on Armed Forced, Strategic Forces Subcommittee, March 25, 2015: p.3, http://docs.house.gov/meetings/AS/AS29/20150325/103106/HHRG-114-AS29-Wstate-WeatheringtonD-20150325.pdf.
[281] Mike Gruss, "U.S. spending on space protection could hit $8 billion through 2020," *SpaceNews,* July 2, 2015, http://spacenews.com/u-s-spending-on-space-protection-could-hit-8-billion-through-2020.

defend itself in space.[282,283] There was also increased focus on preparing to "fight a war in space", even though senior U.S. military leaders expressed no desire to start one.[284,285] A similar shift in tone can also be seen in academic writings from U.S. military journals calling for renewed focus on fighting wars in space and offensive space control.[286],[287] The U.S. Congress also weighed in, calling for a study on how to deter and defeat adversary attacks on U.S. space systems, and specifically the role of offensive space operations.[288]

This shift in rhetoric has been accompanied by changes to the national security space organization. A new facility, originally called the a Joint Interagency Combined Space Operations Center (JICSpOC) and later renamed to the National Space Defense Center (NSDC), was created to improve collaboration between military and intelligence communities to respond to attacks in space and became operational in January 2018.[289] The U.S. Congress also criticized the Air Force for its handling of space programs and forced a debate over reorganizing national security space, potentially by created a separate entity such as a Space Corps.[290]

U.S. Counterspace Budget

Despite this increased rhetoric, the unclassified U.S. national security space budget contains a relatively small amount of funding for dedicated counterspace programs but has seen recent increases. Between fiscal year (FY) 16 and FY17, the total unclassified research, development, testing, and evaluation (RDT&E) budget for counterspace programs increased from $24.1 million to $41.9 million[291], and it increased again in FY18 to $68.38 million[292]. Nearly all of the increase

---

[282] John E. Hyten, "Overcoming Our Space Vulnerabilities," Speech at the Space and Missile Defense Symposium, August 12, 2014, http://www.afspc.af.mil/About-Us/Leadership-Speeches/Speeches/Display/Article/731712/overcoming-our-space-vulnerabilities/.

[283] Bob Work, "Remarks at the Space Symposium," April 12, 2016, https://www.defense.gov/News/Speeches/Speech-View/Article/723498/remarks-at-the-space-symposium/.

[284] Steve Liewer, "'The World is Still a Very Dangerous Place': Gen. Hyten Takes Helm of StratCom at a Time of Increasing Global Tensions," *Omaha World-Herald,* November 4, 2016, http://www.omaha.com/news/military/the-world-is-still-a-very-dangerous-place-gen-hyten/article_6d2e4828-a1ec-11e6-a1d2-5f806ae563fa.html.

[285] "AFSPC Commander Announces Space Enterprise Vision," Air Force Space Command Public Affairs, April 11, 2016, http://www.afspc.af.mil/News/Article-Display/Article/730817/afspc-commander-announces-space-enterprise-vision/

[286] B.T. Cesul, "A Global Space Control Strategy," *Air and Space Power Journal,* November-December 2014: https://www.files.ethz.ch/isn/185638/ASPJ-Nov-Dec-2014Full.pdf.

[287] Adam P. Jodice, Mark R. Guerber, "Space Combat Capability…Do We Have It?" *Air and Space Power Journal,* November-December 2014: https://www.files.ethz.ch/isn/185638/ASPJ-Nov-Dec-2014Full.pdf.

[288] House Resolution 3979 – Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, 113th United States Congress, https://www.congress.gov/bill/113th-congress/house-bill/3979/text.

[289] Shellie-Anne Espinosa, "National Space Defense Center Transitions to 24/7 Operations," Air Force Space Command Public Affairs, January 26, 2018, http://www.afspc.af.mil/News/Article-Display/Article/1423932/national-space-defense-center-transitions-to-247-operations/.

[290] Sandra Erwin, "Congressman Rogers: A Space Corps is 'Inevitable,'" *SpaceNews,* December 2, 2017, http://spacenews.com/congressman-rogers-a-space-corps-is-inevitable/.

[291] Exhibit R-2, RDT&E Budget Item Justification: FY 2018 Air Force, Vol. 2, Program Element: PE 1206421F / Counterspace Systems, May 2017: p. 403, RDT&E Budget Item Justification: FY 2018 Air Force, May 2017: p. 403, http://www.saffm.hq.af.mil/Portals/84/documents/Air%20Force%20Research,%20Development,%20Test%20and%20Evaluation%20Vol-II%20FY18.pdf?ver=2017-05-23-160041-060#page=515.

[292] Exhibit R-2, RDT&E Budget Item Justification: FY 2018 Air Force, Vol. 2, Program Element: PE 1206421F / Counterspace Systems, May 2017: p. 697, http://www.saffm.hq.af.mil/Portals/84/documents/Air%20Force%20Research,%20Development,%20Test%20and%20Evaluation%20Vol-II%20FY18.pdf?ver=2017-05-23-160041-060#page=809.

was to support development of the 10.3 version of the CCS electronic warfare system. The FY18 budget also included $28.8 million to purchase two new 10.2 versions of CCS for active duty Air Force and Air National Guard units.[293] It is possible that additional dedicated counterspace programs, and possibly programs with potential counterspace utility, are funded through the classified budget. The United States also spends nearly $8 billion a year on missile defense capabilities, several of which could have counterspace applications.[294]

The United States has also held multiple wargames and exercises over the last 25 years to practice and refine its counterspace doctrine. The most well-known is the Schriever Wargame, which began in the mid-1990s as a biennial tabletop exercise to look at how advanced space technologies influenced future conflicts in space. In recent years, the Schriever Wargame has become an annual event that also explored policy and strategy issues, diplomatic, economic, military, and information activities, and included participation from a growing number of allied military and commercial partners. The 2017 Schriever Wargame looked at scenario in the year 2027 involving a notional peer space and cyberspace competitor in the Pacific Area of Responsibility, and included participation from Australia, Canada, New Zealand and the United Kingdom.[295] In 2017, the USAF also held the first Space Flag exercise. Modeled after the USAF's Red Flag air combat exercise at Nellis Air Force Base, the Space Flag exercise focused on practicing and training for space warfare.[296] The USAF says it expects to hold future Space Flags biannually.

[293] Exhibit P-40, Budget Line Item Justification: FY 2018 Air Force, Vo. 1, P-1 Line Item Number/Title: CTRSPC. Counterspace Systems, May 2017: volume 1-20, http://www.saffm.hq.af.mil/Portals/84/documents/Air%20Force%20Space%20Procurement%20FY18.pdf?ver=2017-05-23-155547-107#page=60.
[294] *Missile Defense Agency Fiscal Year (FY) 2018 Budget Estimates Overview,* Missile Defense Agency, 17-MDA-9186, May 15, 2017, https://www.mda.mil/global/documents/pdf/budgetfy18.pdf.
[295] "Schriever Wargame 2017 Set to Begin," Air Force Space Command, October 12, 2017, http://www.afspc.af.mil/News/Article-Display/Article/1341443/schriever-wargame-2017-set-to-begin/.
[296] Phillip Swarts, "Air Force Launches 'Space Flag' Exercise Inspired by IMAX-Worthy Red Flag War Games," *SpaceNews,* May 3, 2017, http://spacenews.com/air-force-launches-space-flag-exercise-inspired-by-imax-worthy-red-flag-war-games/.

4 – ISLAMIC REPUBLIC OF IRAN

Assessment

Iran has a nascent space program, building and launching small satellites that have limited capability. Technologically, it unlikely Iran has the capacity to build on-orbit or direct-ascent anti-satellite capabilities, and little military motivations for doing so at this point. Iran has not demonstrated any ability to build homing kinetic kill vehicles, and its ability to build nuclear devices is currently constrained by the Joint Comprehensive Plan of Action. Iran has demonstrated the ability to persistently interfere with the broadcast of commercial satellite signals, although its capability to interfere with military signals is difficult to ascertain.

Specifics

DA-ASAT Technologies

There is no public evidence that Iran has developed, or is developing, a dedicated DA-ASAT capability. However, Iran does have a robust ballistic missile program, including a demonstrated satellite launch vehicle, which could theoretically be used as a DA-ASAT rocket. It would still need to be combined with several other technologies that Iran has not yet tested either.

Iran has several short- and medium-range ballistic missiles, either in operational status or in development, with estimated ranges from 150 km to more than 2,000 km. The longer ranged missiles could theoretically be used as the basis for a DA-ASAT rocket, with a potential ceiling of half their ballistic range. There is no evidence Iran has ever tested its ballistic missiles in this role, nor that it has a program to develop this capability.

There are some who claim Iran is developing the ability to create crude electromagnetic pulse (EMP) weapons by putting nuclear-tipped ballistic missiles on ships. Such weapons, they claim, could be used to conduct surprise attacks on national power grids, or as an indiscriminate ASAT weapon.[297] However, many other experts discount the ability to use a primitive nuclear device in this way,[298] and state that this is a scare tactic designed to promote missile defense.[299]

[297] Paul Bedard, "Expert: Iran Ships a Dry Run for Later Nuclear/EMP Attack; Humiliate Obama," *Washington Examiner*, February 14. 2014, https://www.washingtonexaminer.com/expert-iran-ships-a-dry-run-for-later-nuclearemp-attack-humiliate-obama/article/2544041.
[298] Philip Bump, "Republican Warnings About an Electro-Magnetic Pulse (EMP) Attack, Explained," *The Washington Post*, January 15, 2016, https://www.washingtonpost.com/news/the-fix/wp/2016/01/15/no-you-dont-really-need-to-worry-about-an-emp-attack.
[299] Patrick Disney, "The Campaign to Terrify You About EMP," *The Atlantic*, July 15, 2011, https://www.theatlantic.com/international/archive/2011/07/the-campaign-to-terrify-you-about-emp/241971/.

Figure 12 - Iranian Ballistic Missiles
Image Credit: CSIS[300]

Iran is also developing space launch capabilities. It already possesses a proven space launch vehicle, the Safir rocket, which has been used to place four small satellites into orbit. Iran is developing a more capable SLV known as the Simorgh, but it has experienced significant delays. Simorgh shares some design similarities with the North Korean Unha SLV, and was meant to have been launched in 2010.[301] Its conspicuous absence could mean that its development has been harder than anticipated, or that sanctions on ballistic missile and space technology have limited Iran's ability to get materials it needs, or that there have been test launches that failed and not been reported. In April 2016, the first known test of the Simorgh was reported by U.S. intelligence agencies to have been a "partial success" that did not reach orbit.[302] A second test in July 2017

[300] Center for Security and International Studies, "Iran's Ballistic Missiles," *Missile Threat*, accessed March 21, 2018, https://missilethreat.csis.org/country/iran/.
[301] Center for Security and International Studies, "Simorgh," *Missile Threat*, accessed March 21, 2018, https://missilethreat.csis.org/missile/simorgh.
[302] Bill Gertz, "Iran Conducts Space Launch," *Washington Free Beacon*, April 20, 2018, http://freebeacon.com/national-security/iran-conducts-space-launch/.

was reported by Iranian press to have been a success, but U.S. intelligence officials stated it was a catastrophic failure and no objects reached orbit.[303]

Both the Safir and Simorgh are liquid-fueled rockets. They launch from a single space launch facility after a significant set-up period, making them not ideal as counterspace launch vehicles.

Co-Orbital Technologies

Iran has no known co-orbital ASAT capabilities or development program, and its indigenous satellite manufacturing and operations capabilities are very basic. Iran has put a small number of low-mass satellites on orbit using the Safir SLV. Its pace of launch attempts is slow, possibly due to the effect of sanctions on its ability to make progress, perhaps because they are sensitive to international reaction to launches because of their similarities to ballistic missile launch. Iran has launched four satellites into orbit: Omid (2009),[304] Rasad (2011),[305] Navid (2012),[306] and Fajr (2015).[307]

These were all small satellites, 50 kg or lighter, lofted into such low-altitude orbits that atmospheric drag brought them down within weeks. No data have been published from their satellites, so either they did not work as anticipated or they worked but the results were not impressive and judged not to improve the reputation of the program. Iran does have plans to launch larger satellites,[308] both domestically-developed and through bilateral cooperation with other countries, but many of those plans have been significantly delayed. Iran recently announced that it will attempt to launch its Nahid-2 communications satellite before the end of 2018.[309]

Iran has not demonstrated the ability to manufacture satellites with significant on-orbit maneuverability or remote sensing capabilities, nor the ability to successfully do the precision command-and-control (C2), that would be necessary to develop an effective co-orbital ASAT capability.

Electronic Warfare

There is significant public evidence that Iran has the ability to conduct electronic warfare attacks against commercial satellite broadcasters. Specifically, Iran been accused of repeatedly interfering

---

[303] "Iran Announces First Successful Simorgh Test Launch," *SpaceFlight101.com*, July 29, 2017, http://spaceflight101.com/iran-announces-first-successful-simorgh-test-launch/.
[304] Robert Tait, "Iran Launches First Domestically Produced Satellite," *The Guardian*, February 3, 2009, https://www.theguardian.com/world/2009/feb/03/iran-satellite-launch-omid.
[305] David Wright, "Radad-1: Iran Launches Its Second Satellite," *All Things Nuclear*, June 16, 2011, https://allthingsnuclear.org/dwright/rasad-1-iran-launches-its-second-satellite.
[306] David Wright, "Another Iranian Satellite Launch: Navid," *All Things Nuclear*, February 6, 2012, https://allthingsnuclear.org/dwright/another-iranian-satellite-launch-navid.
[307] "Iran's Safir Rocket Successfully Launches Fajr Satellite Into Orbit," *SpaceFlight101.com*, February 2, 2015, http://www.spaceflight101.net/irans-safir-rocket-successfully-launches-fajr-satellite-into-orbit.html.
[308] Ahmad Majidyar, "Iran Plans to Launch Several Satellites Into Space, Including 1st Sensor-Operational Satellite," *Middle East Institute*, May 30, 2017, http://www.mei.edu/content/io/iran-plans-launch-several-satellites-space-including-1st-sensor-operational-satellite.
[309] "Iran Announces Launch of Nahid-2 Communications Satellite for 2018," *SpaceWatch Middle East*, May 2017, https://spacewatchme.com/2017/05/iran-announces-launch-nahid-2-communications-satellite-2018/.

with commercial communications satellites' ability to broadcast Persian-language programming into Iran over the last several years. In some cases, it appears Iran coordinated with other States to perform the jamming. For example, the jamming of Telstar 12's broadcast of Persian-language content originating from California was jammed from Havana, Cuba, started in 2003, and eventually similar jamming occurred from Bulgaria and Libya in 2005/2006.[310] Eventually, it appears, Iran became able to jam these channels from within its own territory.

In 2010, the International Telecommunication Union (ITU) ordered Iran to assist in stopping the jamming originating from its territory, saying that it was acting on two complaints from Eutelsat that its broadcasts of Persian language programs by the BBC and the Voice of America have been interfered with.[311]

There is also speculation that Iran may have more advanced electronic warfare capabilities that could interfere with satellite-based command and control signals or GPS signals. In late 2011, a stealthy U.S. RQ-170 Sentinel UAV landed in Iran.[312] The United States confirmed that a UAV had landed in Iran and asked for its return.[313] The UAV was reportedly part of an intelligence operation near the Iran-Afghanistan border and there had been no intent for it to land in Iran.

The United States first suggested that the UAV crash-landed because of a technical malfunction and then because of pilot error. Iran claims that it took command of the UAV and brought it down with little damage. Because these UAVs fly at high altitudes and are stealthy, and was displayed largely in one piece, it is unlikely that it was shot down. It is also unlikely that Iran took control of the UAV: C2 of such a UAV would typically be done over encrypted military satellite channels that would require extremely sophisticated capabilities to hijack.

Some reporting suggests that instead of gaining direct control of the UAV, Iranian electronic warfare specialists used a combination of techniques to bring it down. The attack would have started by interrupting C2 communications with the UAV. Reportedly, under these circumstances, a drone would be programmed to return to its home base. In an interview, an Iranian engineer claims that Iran then faked or spoofed GPS coordinates so that the drone would land in Iran, not at its home based in Afghanistan [314] While the ability to conduct such a spoofing attack on the civil GPS signal has been demonstrated,[315] conducting a similar attack on the military GPS signal would

---

[310] "Satellite Jamming in Iran: A War Over Airwaves," *Small Media Lab*, November 2012, https://smallmedia.org.uk/sites/default/files/Satellite%20Jamming.pdf.
[311] "UN tells Iran to stop jamming int'l broadcasts," *Associated Press*, March 26, 2010.
[312] Greg Jaffe and Thomas Erdbrink, "Iran Says It Downed U.S. Stealth Drone; Pentagon Acknowledges Aircraft Downing," *The Washington Post*, December 4, 2011, https://www.washingtonpost.com/world/national-security/iran-says-it-downed-us-stealth-drone-pentagon-acknowledges-aircraft-downing/2011/12/04/gIQAyxa8TO_story.html.
[313] Rick Gladstone, "Iran is Asked to Return U.S. Drone," *The New York Times*, December 12, 2011, http://www.nytimes.com/2011/12/13/world/middleeast/obama-says-us-has-asked-iran-to-return-drone.html.
[314] Scott Peterson and Payam Faramarzi, "Exclusive: Iran Hijacked U.S. Drone, Says Iranian Engineer," *Christian Science Monitor*, December 15, 2011, https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer/.
[315] "Spoofing a Superyacht At Sea," *The University of Texas at Austin*, July 30, 2013, https://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea

be much more challenging because it is encrypted. It is possible that Iran may have found a way to jam the military GPS signal, forcing the UAV to fall back on the civil signal. Subsequent to the capture of the sophisticated drone, Iran claims to have been able to break into encrypted data on-board the drone, gaining access to sensitive information about the program, but this is difficult to confirm from public sources.[316]

Potential Military Utility

Iran's current counterspace capabilities likely have very limited military utility. Iran's current efforts appear focused on electronic warfare and cyber attacks, and not on kinetic counterspace capabilities. Its current satellites are very short-lived, and without sophisticated rendezvous and proximity technology or C2 capabilities, it is extremely unlikely Iran could command a co-orbital ASAT to deliberately collide with another satellite with any degree of certainty. The best it could hope for would be to increase the possibility of a risk of collision to a degree that might force its adversary to alter the trajectory of their satellite. Iran is not known to possess the technology for a kinetic-kill vehicle that would be capable of a DA-ASAT attack. If Iran is able to produce a working nuclear weapon, can miniaturize it, develops a ballistic missile or SLV that can carry it, and can mate the two, it is possible to conduct a crude EMP attack against LEO satellites. However, it would be extremely difficult to direct such an attack against specific satellites, and most U.S. military satellites are hardened against radiation and EMP effects. Such an attack would also have indiscriminate effects against many other non-military satellites in LEO.[317]

[316] John Hudson, "Nobody Knows if Iran's Drone Hack Was a Hoax," *The Atlantic*, April 24, 2012, https://www.theatlantic.com/international/archive/2012/04/nobody-knows-if-irans-drone-hack-was-hoax/328944/.
[317] "Collateral Damage to Satellites from an EMP Attack," Defense Threat Reduction Agency, August 2010, http://www.dtic.mil/dtic/tr/fulltext/u2/a531197.pdf.

5 – DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA

Assessment

North Korea, officially known as the Democratic People's Republic of Korea (DPRK), has no demonstrated capability to mount kinetic attacks on space assets; neither with a direct ascent ASAT nor a co-orbital system.

In its official statements, North Korea has never mentioned anti-satellite operations or intent, suggesting that there is no clear doctrine guiding Pyongyang's thinking at this point. North Korea does not appear motivated to develop dedicated counterspace assets, though certain capabilities in their ballistic missile program might be eventually evolved for such a purpose.

The DPRK has demonstrated the capability to jam civilian GPS signals within a limited geographical area. Their capability against U.S. military GPS signals is not known. There has been no demonstrated ability of the DPRK to interfere with satellite communications, although their technical capability remains unknown.

Specifics

The North Korean ballistic missile program traces its start back to the 1980s with the acquisition of Soviet-era Scud technology. At present, no dedicated ASAT program exists separate from the country's ballistic missile programs. North Korean systems comprise two primary components: rapidly maturing ground-launched ballistic missile capabilities and the development of some radar systems.

DA-ASAT Technologies

North Korea has multiple ballistic missiles systems, including those in the intermediate range ballistic missile (IRBM) and ICBM class, which could possibly be used as the basis for future DA-ASAT capabilities. The first is the Pukguksong family of IRBMs, which include the KN-11 (Pukkuksong-1) and the KN-15 (Pukkuksong-2). The KN-11 is a two-stage solid-fuel SLBM with a purported range of 500-2,500 km, while the KN-15 is the land-based variant. North Korea conducted a successful cold-launched test of the KN-15 in May 2017.[318]

The Hwasong-10 (Musudan) is an IRBM reportedly modeled off of the Soviet R-27/SS-N-6 missile system. The system is liquid-fueled with a maximum range of 3,500 km. The Musudan has a spotty testing record, but the sixth test of the system reportedly was a success.[319]

The Hwasong-12 (KN-17) is a newer ballistic missile, tested May 14, 2017, August 28, 2017, and September 14, 2017, using liquid propellant and a high-thrust engine and mounted on a TEL. An

[318] Ankit Panda, "North Korea has Tested a New Solid-Fuel Missile Engine," *The Diplomat*, October 25, 2017, https://thediplomat.com/2017/10/north-korea-has-tested-a-new-solid-fuel-missile-engine/.
[319] Ankit Panda, "North Korea's Musudan Missile Test Actually Succeeded. What Now?" *The Diplomat*, June 23, 2016, https://thediplomat.com/2016/06/north-koreas-musudan-missile-test-actually-succeeded-what-now.

additional, possibly ICBM-relevant flight test, using a similar engine to the KN-17, was conducted in March. This was possibly just a larger variant of the existing Hwasong-10 IRBM, but the test indicates the ability to comfortably overshoot Guam and reach lower satellite orbital altitudes. The Hwasong-12 is presumed to be a one-stage missile with a range of 3,700-4,500 km.[320]

Kim Jong Un announced in the annual 2017 New Year's Address that the country was nearly ready to flight-test an ICBM.[321] There have since been two ICBM tests in 2017 of a relatively new system, the Hwasong-14. North Korea tested the Hwasong-14 (KN-20) on July 4, 2017, and July 28, 2017, using a lofted trajectory. Several estimates place the range around 10,000 km, placing American cities and targets in space above LEO potentially at risk.[322] The Hwasong-14 is a two-stage liquid fuel design.

The Hwasong-15 (KN-22) was launched for the first time on November 29, 2017, when this liquid-fueled ICBM flew on a lofted trajectory to an altitude of 4,500 km.[323] If flown on a standard trajectory, it could have a feasible reach of 13,000 km, which, according to David Wright of the Union of Concerned Scientists, "is significantly longer than North Korea's previous long range tests."[324] According to North Korea's Korean Central News Agency (KCNA), this flight test was of "an intercontinental ballistic rocket tipped with super-large heavy warhead" which could reach "the whole mainland of the U.S."[325]

North Korea has other presumed ICBM-range systems that have not yet been flight-tested or deployed. The first is the Hwasong-13 (KN-08), a three-stage road-mobile ICBM first seen in the 2012 military parade, and a variant of this missile known as the KN-14, shortened to two stages. These are alleged road-mobile ICBMs displayed in past military parades but have not yet been flight-tested or deployed.[326]

North Korea's only known operational satellite launch vehicle is the Unha-3. It appears to derive design components from the Taepodong-2, which was originally believed by U.S. intelligence to be a possible ICBM.[327] Although operational, the reliability of the Unha-3 is not assured. The TD-

[320] Jeffrey Lewis, "North Korea's Hwasong-12 Missile: Stepping Stone to an ICBM," Nuclear Threat Initiative, July 20, 2017, http://www.nti.org/analysis/articles/north-koreas-hwasong-12-missile-stepping-stone-icbm/.
[321] Choe Sang-hun, "Kim Jong-un Says North Korea is Preparing to Test Long-Range Missile," *The New York Times*, January 1, 2017, https://www.nytimes.com/2017/01/01/world/asia/north-korea-intercontinental-ballistic-missile-test-kim-jong-un.html.
[322] David Wright, "North Korean ICBM Appears Able to Reach Major U.S. Cities," *Union of Concerned Scientists*, July 28, 2017, http://allthingsnuclear.org/dwright/new-north-korean-icbm; and, Ankit Panda and Vipin Narang, "North Korea's ICBM: A New Missile and a New Era," *The Diplomat*, July 7, 2017, https://thediplomat.com/2017/07/north-koreas-icbm-a-new-missile-and-a-new-era.
[323] Ankit Panda, "The Hwasong-15: The Anatomy of North Korea's New ICBM," *The Diplomat*, December 6, 2017, https://thediplomat.com/2017/12/the-hwasong-15-the-anatomy-of-north-koreas-new-icbm/.
[324] David Wright, "North Korea's Longest Missile Test Yet," *All Things Nuclear* blog, November 28, 2017, http://allthingsnuclear.org/dwright/nk-longest-missile-test-yet.
[325] Ankit Panda, "The Hwasong-15: The Anatomy of North Korea's New ICBM," *The Diplomat*, December 6, 2017, https://thediplomat.com/2017/12/the-hwasong-15-the-anatomy-of-north-koreas-new-icbm/.
[326] Jeffrey Lewis, "New DPRK ICBM Engine," Arms Control Wonk, April 9, 2016, http://www.armscontrolwonk.com/archive/1201278/north-korea-tests-a-fancy-new-rocket-engine/.
[327] John Schilling, "Where's That North Korean ICBM Everyone Was Talking About?" *38 North*, March 12, 2015, https://www.38north.org/2015/03/jschilling031215/.

2 failed in several tests throughout the 2000s, raising some questions regarding both its relationship to the Unha-3 and the latter's reliability. The first attempt to use the Unha-3 to launch the Kwangmyŏngsŏng 3 satellite in April 2012 resulted in failure, but in December 2012 the Unha-3 successfully placed the first North Korean satellite (Kwangmyŏngsŏng 3-2) in orbit.[328] The Unha-3 was used to put the second satellite (Kwangmyŏngsŏng 4) into orbit in 2016.[329]

The Unha-3 is known to be a multi-stage rocket with liquid propellant requiring conventional launch pad and extensive visible preparations. The first stage consists of four Nodong engines, making it too large for mobile use.[330]

Aside from the active ballistic missile and SLV programs, North Korea also has active solid motor and liquid fuel programs and uses both in active missile systems and in development tests. Work is underway on the creation of more advanced rocket engines. This has been evidenced in attempts to create a compact SLBM with two Hwasong-10 engines, similar to that in the Soviet R-27 SLBM, in a single stage, and known now as the March-18 engine after testing at the Sohae Satellite Launch Center. The March-18 engine in particular is intended as a "high-thrust engine [to] help consolidate the scientific and technological foundation to match the world-level satellite delivery capability in the field of outer space development."[331]

Some have speculated that North Korea could be able to combine a ballistic missile and a nuclear warhead into an EMP weapon, targeted against either U.S. satellites or domestic infrastructure. However, it seems unlikely at this point that North Korea would dedicate one of its limited nuclear warheads to an unproven task.[332] Additionally, it is unknown how large of a yield from a nuclear warhead is necessary to affect the U.S. electrical grid.[333] Although North Korea likely has demonstrated a thermonuclear capability as of March 2018, the country's nuclear warheads do not approach the megaton range yield that would likely be necessary. Additionally, North Korea's ICBM force, while growing in technical sophistication and performance, is not currently capable of carrying such a heavy warhead. Historical nuclear tests, such as the U.S. Starfish Prime test in 1962, are known to have generated effects that damaged or destroyed satellites in orbit at the time.[334] However, it would be difficult to predict the ability of creating such effects against military satellites, particularly since many U.S. military satellites are hardened against radiation and EMP effects.

---

[328] Center for Strategic and International Studies, "Taepodong-2 (Unha-3)," https://missilethreat.csis.org/missile/taepodong-2/.
[329] Andrea Shalal and Idrees Ali, "North Korea Satellite Tumbling in Orbit Again: U.S. Sources," *Reuters*, February 18, 2016, http://www.reuters.com/article/us-northkorea-satellite/north-korea-satellite-tumbling-in-orbit-again-u-s-sources-idUSKCN0VR2R3.
[330] Center for Strategic and International Studies, "Taepodong-2 (Unha-3)," https://missilethreat.csis.org/missile/taepodong-2/.
[331] "Kim Jong Un Watches Ground Jet Test of Newly Developed High-Thrust Engine," *Korean Central News Agency*, March 19, 2017, http://www.kcna.co.jp/item/2017/201703/news19/20170319-01ee.html.
[332] Jeffrey Lewis, "Welcome to the Thermonuclear Club North Korea," *Foreign Policy*, September 4, 2017, http://foreignpolicy.com/2017/09/04/welcome-to-the-thermonuclear-club-north-korea/.
[333] Kyle Mizakomi, "North Korea Can't Kill Ninety Percent of Americans," *Popular Mechanics*, March 3, 2017, http://www.popularmechanics.com/military/weapons/a25883/north-korea-cant-kill-ninety-percent-of-americans/.
[334] Richard Hollingham, "The Cold War nuke that fried satellites," *BBC News*, September 11, 2015, http://www.bbc.com/future/story/20150910-the-nuke-that-fried-satellites-with-terrifying-results.

Co-Orbital ASAT Technologies

North Korea currently possess a very rudimentary satellite development and command and control capability, but they have not demonstrated any of the rendezvous and proximity operations or active guidance capabilities necessary for a co-orbital satellite capability.

There are currently six objects in orbit as a result of two North Korean space launches. Two of these objects are satellites. The first successful launch of a satellite into orbit occurred in December 2012 from the Sohae Satellite Launching Station. Initial reports at the time suggested that the satellite, along with a third-stage rocket body and two small pieces of associated debris, were placed into orbit, but that the satellite was "spinning out of control" and there were no ultra-high frequency (UHF) radio signals detected from the satellite. This suggest the satellite was either not under any stabilization or was not functional after deployment.[335] However, the satellite was still following a relatively predictable orbital trajectory and did not pose a collision threat to other space objects.

North Korea launched a second satellite in February 2016, named Kwangmyongsong-4.[336] Both the rocket body and the satellite (pictured below) entered into a stable orbit. As with the 2012 satellite, this satellite was purported to be for earth observation purposes.[337] The 2016 version reportedly weighed almost twice as much as the 2012 satellite, at around 200 kg.[338] The satellites and associated objects are in a normal and predictable orbit and do not pose a significant collision threat to other space objects.

[335] Brian Weeden, "Almost Everything You've Heard About the North Korean Space Launch Is Wrong," *Wired*, December 18, 2012, https://www.wired.com/2012/12/launch/.
[336] Melissa Hanham, "Highlights and Initial Thoughts from the DPRK Launch," *Arms Control Wonk*, February 7, 2016, http://www.armscontrolwonk.com/archive/1200997/highlights-and-initial-thoughts-from-the-dprk-launch.
[337] Anna Fifield, "North Korea Launches 'satellite,' Sparks Fears About Long-Range Missile Program," *Washington Post*, February 6, 2016, https://www.washingtonpost.com/world/north-korea-launches-satellite-sparks-fears-about-long-range-missile-program/2016/02/06/0b6084e5-afd1-42ec-8170-280883f23240_story.html?utm_term=.55ccd928b712.
[338] Michael Elleman, "North Korea Launches Another Large Rocket: Consequences and Options," *38 North*, February 10, 2016, http://www.38north.org/2016/02/melleman021016.

Figure 13 - Kwangmyongsong-4
Two views of the purported earth-observation satellite Korea launched in January 2016. Image credit: Chinaspaceflight.com.[339]

Neither of the two Kwangmyŏngsŏng satellites is considered to be operational. Both are thought to have failed soon after launch. This is evidenced by the lack of detected signals and instability of the platforms. Kwangmyŏngsŏng 3-2 was reported to be tumbling on December 17, 2012, five days after launch, and Kwangmyŏngsŏng 4 was reported to be tumbling as early as February 9, 2016, only three days after launch. [340] The satellites can be determined to be tumbling by space tracking radars systems, or even by amateur astronomers observing periodic variations of the intensity of the light reflected from the sun as the objects pass over observers near local dawn and dusk.

Although both satellites were announced as remote sensing systems, it is doubtful if they conducted much sensor activity due to their early failures. The North Korean satellite expertise is considered to be rudimentary, with the payloads likely being capable of only producing low resolution imagery at best, and it is doubtful if either of the two satellites would have been militarily useful, even had they not failed prematurely.

There is no indication that the Kwangmyŏngsŏng series of satellites had any counterspace capability nor that there is any indication of intent, on the part of North Korea, to attempt to develop such a capability. Neither of the satellites conducted orbital maneuvers.[341] Any serious attempt at orbital counterspace would require a sophistication that is far beyond the capacity of North Korea for the foreseeable future.

---

[339] "North Korea successfully launches the Star 4 satellite using the light star rocket at 08:30 of February 7th," *chinaspaceflight.com*, February 11, 2016, https://www.chinaspaceflight.com/default/DPRK-201602.html.
[340] David Todd, "Kwangmyongsong 3-2 is in orbit but is "tumbling" and not transmitting", *Seradata*, December 17, 2012, https://www.seradata.com/kwangmyongsong_3-2_is_in_orbit/; Nash Jenkins, "North Korea's Satellite Is Tumbling in Orbit", *Time*, February 9, 2016, http://time.com/4213428/north-korea-satellite-tumbling/.
[341] TLEs for the Kwangmyŏngsŏng satellites are available from the Space Track web site (https://www.space-track.org/auth/login). Orbital maneuvers can be detected from the TLE data.

Electronic Warfare

On numerous occasions, North Korea has demonstrated the capability to interfere with civilian GPS navigation used by passenger aircraft, automobile, and ship systems in the vicinity of the South-North border and nearby coastal areas.[342] This type of interference (downlink jamming) targets GPS receivers within range of the source of the jamming signal but has no impact on the GPS satellites themselves nor the service provided to users outside the range of the jammers. The area affected will depend on the power emitted by the jammer and the local topography. In the case of the reported North Korean incidents, the range was estimated to be several tens of kilometers.

According to unnamed U.S. officials, this type of jamming would not affect U.S. military members who use the military GPS signals.[343] The GPS interference incidents along the South-North border appear to have been deliberately targeting civilian receivers, presumably as part of a North Korean political strategy or tactic. Some events have coincided with joint South Korea - U.S. military exercises. North Korea could also be developing jammers that are effective against the military GPS signals, but to date there is no public evidence of such development, testing, or use.

There is no public information indicating North Korea has the ability to jam satellite communications. North Korea does routinely jam terrestrial broadcasts from foreign sources, such as the BBC, Voice of America, Radio Free Asia and South Korea's KBS, to prevent their citizens from listening,[344] but there is no public information on the DPRK's capabilities to jam satellite broadcasts. It is assessed that uplink jamming of communication satellites have not, or rarely, occurred since that would likely have been reported by the targeted satellite operators. Downlink jamming, which affects only the receivers in a local area, may be occurring within North Korea, but there is no information available on that.

Policy/Doctrine

As of yet, there is no clear doctrine for counterspace weapons in the DPRK. In fact, there is a curious absence of discussion on counterspace weapons in the DPRK state media. Surveying the

[342] "North Korea 'jamming GPS signals' near South border," *BBC News*, April 1, 2016, http://www.bbc.com/news/world-asia-35940542.
[343] "Pentagon concerned about North Korea jamming GPS signals, officials say", *Fox News US,* April 6, 2016, http://www.foxnews.com/us/2016/04/06/pentagon-concerned-about-north-korea-jamming-gps-signals-officials-say.html.
[344] Julian Ryall, "North Korea 'aggressively' jamming BBC's new Korean-language service", *The Telegraph*, September 27, 2017, https://www.telegraph.co.uk/news/2017/09/27/north-korea-aggressively-jamming-new-bbc-broadcasts/.

archives since 2010 does not reveal a single mention of ASAT or counterspace. Satellites and space are only mentioned in the context of peaceful programs in the DPRK parlance.[345]

[345] Most state media references to space cite DPRK efforts to successfully launch satellites, ostensibly for earth observation purposes. These references discuss the development of high-thrust engines (usually referenced as the March 18th engine) for delivery of satellites into orbit, and the development of the earth observation satellite technology (only EO satellites so far (Kwangmyongsong-4), launched in 2016). See: "Kim Jong Un Watches Ground Jet Test of Newly Developed High-Thrust Engine," *Korean Central News Agency*, March 19, 2017. Thus far, official statements from North Korea have emphasized space as a common good: "Space is wealth common to man," and have emphasized peaceful uses. "Peaceful Development and Use of Space Are Legitimate Right of Sovereign State: DPRK Delegation," *Rodong Sinmun*, June 21, 2017. State media also references work on meteorological atmospheric observation systems, which may have some applications for radar tracking systems. See: "A Breakthrough," *Naenara News*, July 12, 2015.

6 – REPUBLIC OF INDIA

Assessment

India has over five decades of experience with space capabilities, but most of that has been civil in focus. It is only in the past several years that India has started organizationally making way for its military to become active users and creators of its space capabilities. India's military has been developing an indigenous missile defense program that its supporters argue could provide a latent ASAT capability, should the need arise; this capability has not been tested. It is possible that India would move into rapidly testing an ASAT if it felt that the international community was getting close to creating an international legal regime banning kinetic ASAT tests; otherwise, given how much investment the Indian military is making in its satellite capacity and the income that Indian rockets are making launching other countries' satellites, it is unlikely that they will move to actively create an official counterspace program.

Specifics

DA-ASAT Technologies

India launched its first rocket - a US-supplied Nike-Apache - in November 1963.[346] In July 1980, with the Rohini RS-1 satellite, India became the 7th nation to have indigenous satellite launch capabilities.[347]

India's space program was at first primarily focused on peaceful uses and development. However, as more countries incorporated space into security capabilities, this became more attractive to India as well. China had its first successful intercept by an anti-satellite weapon in 2007, which generated space debris and worries globally about its military space capacity. Indian officials operating in the context of historically fraught Indo-Chinese relations including a war in 1962, ongoing border disputes, and concerns about China's role in the Asia-Pacific, began to consider whether India should have its own ASAT capability. Lt. General H S Lidder, then Integrated Defense Staff chief, was quoted as saying, "[W]ith time, we will get sucked into the military race to protect space assets and inevitably there will be a military contest in space. In a life-and-death scenario, space will provide the advantage."[348]

---

[346] Amrita Shah, "Flashback 1963: The beginnings of India's dazzling space programme; An excerpt from Amrita Shah's 'Vikram Sarabhai – A Life', about the father of India's space initiatives," *Scroll.In*, February 15, 2017, https://scroll.in/article/829466/flashback-1963-the-beginnings-of-indias-dazzling-space-programme.

[347] "List of Indian Satellites," Wikipedia.org, https://en.wikipedia.org/wiki/List_of_Indian_satellites, last updated March 10, 2018.

[348] Harsh Vasani, "India's Anti-Satellite Weapons: Does India truly have the ability to target enemy satellites in war?" *The Diplomat*, June 14, 2016, http://thediplomat.com/2016/06/indias-anti-satellite-weapons/.

Dr K. Kasturirangan, former head of the Indian Space Research Organization (ISRO), said in September 2009 that "India has spent a huge sum to develop its capabilities and place assets in space. Hence, it becomes necessary to protect them from adversaries. There is a need to look at means of securing these."[349] Air Chief Marshal P.V. Naik said in February 2010, "Our satellites are vulnerable to ASAT weapon systems because our neighborhood possesses one."[350]

In February 2010, V.K. Saraswat, who at that time was the head of India's Defense Research and Development Organization (DRDO), stated, "In Agni-III, we have the building blocks and the capability to hit a satellite but we don't have to hit a satellite," due to debris concerns; instead, India "will validate the anti-satellite capability on the ground through simulation."[351] In 2012, Saraswat asserted, "Today, India has all the building blocks for an anti-satellite system in place. We don't want to weaponize space but the building blocks should be in place. Because you may come to a time when you may need it.... We will not do a physical test (actual destruction of a satellite) because of the risk of space debris affecting other satellites."[352] He went on to say that the Long Range Tracking Radar used for Indian missile defense had a range of 600 km, but that it could be extended to 1,400 km in order to track satellites in orbit, and noted the work done on the BMD system's communications and kill vehicles.[353] In promoting the Agni-V ICBM, he pointed out that "An ASAT weapon would require to reach [sic] about 800 km altitude... Agni V gives you the boosting capability and the 'kill vehicle', with advanced seekers, will be able to home into the target satellite," but again iterated that, "India does not believe in weaponization of space. We are only talking about having the capability. There are no plans for offensive space capabilities."[354]

India's missile defense system was intended to have two phases: one that would intercept an intermediate range ballistic missile (IRBM), a capability that initially was planned to be in place around 2012/2013, and one that would intercept an intercontinental ballistic missile (ICBM), a capability that initially was planned to be in place around 2016. The first phase's interceptors were the Prithvi Air Defense (PAD) system (later to be replaced by the Prithvi Defense Vehicle, or PDV) and the Advanced Area Defense (AAD) system; the second phase would use the AD1 missile. The PDV was successfully test-fired in February 2017 and is intended to provide exoatmospheric intercepts; it was reported to have destroyed its target at an altitude of 97 km.[355]

---

[349] "Ex-ISRO chief calls China's A-SAT a cause for worry," *Press Trust of India*, September 14, 2009.
[350] Bharath Gopalaswamy and Harsh Pant, "Does India need anti-satellite capability?" *Rediff News*, February 9, 2010, http://news.rediff.com/column/2010/feb/09/does-india-need-anti-satellite-capability.htm.
[351] "India has anti-satellite capability: Saraswat," Press Trust of India, February 10, 2010.
[352] Sandeep Unnithan, "'India has all the building blocks for an anti-satellite capability:' DRDO chief Dr Vijay Kumar Saraswat explains why Agni-V is a technological breakthrough and how it gives India the capability to target satellites in space," *India Today,* April 27, 2012, http://indiatoday.intoday.in/story/agni-v-drdo-chief-dr-vijay-kumar-saraswat-interview/1/186248.html.
[353] Unnithan, "India has all the building blocks."
[354] Rajat Pandit, "After Agni-V launch, DRDO's new target is anti-satellite weapons," *Times of India*, April 21, 2012, http://timesofindia.indiatimes.com/india/After-Agni-V-launch-DRDOs-new-target-is-anti-satellite-weapons/articleshow/12763074.cms.
[355] "India successfully test-fires interceptor missile," *Times of India,* February 11, 2017, http://timesofindia.indiatimes.com/india/india-successfully-test-fires-interceptor-missile/articleshow/57093816.cms.

The AAD was launched in March 2017 to make a successful intercept at an altitude of 15-25 km.[356] India is also in talks to buy Russia's S-400 air defense system for $5 billion, but that purchase has not been officially completed.[357] India's missile defense network uses the Green Pine radar, which was developed by Israel as part of its Arrow missile defense system.

Whether India would actively test an official ASAT system is unlikely, although distantly possible, if Indian officials believe that the international community is close to establishing some sort of kinetic energy ASAT ban; they might decide to hold a test so that they could be grandfathered in as an established ASAT actor. Indian officials are still upset that India was left out of the Nuclear Non-Proliferation Treaty (NPT) as a non-nuclear weapon state and believe, probably rightfully so, that if they had tested a nuclear weapon prior to the treaty's 1968 inception (as opposed to when they did test it, in 1974), they would have been grandfathered in to be a nuclear weapons state, and have taken that lesson to heart.

Does India have the technical capacity to hold an ASAT test? It has made many strides in its tracking and situational awareness capabilities. It currently has ground stations in Brunei, Biak (Indonesia), Mauritius, and the Andaman and Nicobar Islands for tracking satellites, and is building a satellite tracking and data reception center in Vietnam.[358] There have also been talks about possibly signing a space situational awareness agreement with the United States, but that has not been completed yet. Perhaps the more relevant question is, what would India target if it wanted to hold an ASAT test? And if it were held at an altitude that allowed the debris to de-orbit quickly enough, would that be sufficient to avoid international criticism? A test that would strive for a close approach (but deliberate miss) to the target satellite would be very tricky to model and require great confidence in the calculations and situational awareness of the target. Rajaram Nagappa did an analysis of how India might go ahead with an ASAT test, if it made the decision to do so; he noted that because most of India's satellites are not in very low Earth orbit, India would have to create a satellite and launch it for this purpose. Nagappa commented, "The mission and its outcome has to be traded off with the cost, effort, and time required for achieving a low orbit satellite."[359]

India's space vehicle launchpad is at Satish Dhawan Space Center near Sriharikota (See Satish Dhawan, Section 8-14). Officials announced in August 2017 that work has begun on a second

[356] "Successful Test Firing of AAD Endo-Atmospheric Interceptor Missile," Press Information Bureau, Government of India, Ministry of Defence, March 1, 2018, http://pib.nic.in/newsite/PrintRelease.aspx?relid=158774.
[357] Vivek Raghuvanshi, "India, Russia fail to finalize S-400 air-defense deal," *Defense News*, January 23, 2018, https://www.defensenews.com/global/asia-pacific/2018/01/23/india-russia-fail-to-finalize-s-400-air-defense-deal/.
[358] "India building satellite tracking station in Vietnam to track China's movements in South China sea," *Catch News,* February 14, 2017, http://www.catchnews.com/world-news/india-is-building-a-satellite-tracking-station-in-vietnam-to-track-china-s-movements-in-the-south-china-sea-1453791004.html.
[359] Rajaram Nagappa, "Emerging Space Technologies – Their Impact on National Security," in *Space Security: Need for Global Convergence*, ed. Arvind Gupta, Amitav Mallik, Ajey Lele, (New Delhi: Institute for Defence Studies and Analyses, 2012), p. 97.

vehicle assembly building at the center that is anticipated to be completed by mid-2018.[360] According to A S Kiran Kumar, ISRO chairperson, "With the new assembly facility, we will be able to assemble parallelly the launch vehicle and bring it to existing two launchpads. It will thus help boost the launch capability of the Sriharikota centre."[361] Launches from the center are expected to increase from seven a year to 12 a year.[362]

Policy/Doctrine

India currently does not have a national space policy, although one has been rumored to be in the works for years and being developed by ISRO. It is thought by supporters that the strategic ambiguity by not having a policy is more effective than actually having something specific. Its Constitution from 1950, Satellite Communications Policy from 2000, and revised Remote Sensing Data Policy from 2011 are the only national laws that specifically deal with space. Under consideration is a draft Geospatial Information Regulation Bill from 2016.[363]

In October 2007, the Defence Space Vision was released, and listed intelligence, surveillance, reconnaissance, communication, and navigation as primary thrust areas.[364] In 2010, the Ministry of Defense wrote a "Technology Perspective and Roadmap" which discussed developing ASATs for "for electronic or physical destruction of satellites (2,000 km altitude above earth's surface) and GEO-synchronous orbits." [365]

There is no separate space force for the Indian armed forces, which are comprised of the Army, Navy, and Air Force. In June 2010, India established an Integrated Space Cell, located in the Integrated Defense Headquarters, which is comprised of all three branches of India's armed forces.[366] The Integrated Space Cell is supposed to be in charge of defense-specific space capability requirements and is composed of the armed forces, the Department of Space, and ISRO. When announcing the cell, Antony stated that part of why India needed it was "[o]ffensive counter-space systems like anti-satellite weaponry, new classes of heavy-lift and small boosters and an improved array of military space systems have emerged in our neighborhood."[367] There has been talk by the Ministry of Home Affairs of a "Border Space Command," that would use space

[360] "ISRO readying for a number of launches," *Deccan Chronicle*, January 27, 2018, https://www.deccanchronicle.com/science/science/270118/isro-readying-for-a-number-of-launches.html.
[361] Surendra Singh, "Isro's launch capacity will get boost with new facility at Sriharikota by year-end," *Times of India*, August 3, 2017, http://timesofindia.indiatimes.com/india/isros-launch-capacity-will-get-boost-with-new-facility-at-sriharikota-by-year-end/articleshow/59890384.cms.
[362] Singh, "Isro's launch capability will get boost."
[363] Senjuti Mallick, "Why India Needs a Space Law," *The Hindu*, June 17, 2017, http://www.thehindu.com/opinion/open-page/why-india-needs-a-space-law/article19094453.ec
[364] Rajat Pandit, "Dedicated satellite for Navy by year-end," *The Times of India*, May 10, 2010.
[365] Pandit, "After Agni-V launch."
[366] Rajeswari Pillai Rajagopalan, "Need for an Indian Military Space Policy," in *Space India 2.0: Commerce, Policy, Security and Governance Perspectives*, ed. Rajeswari Pillai Rajagopalan and Narayan Prasad (Observer Research Foundation, 2017), http://cf.orfonline.org/wp-content/uploads/2017/02/ORF_Space-India-2.0.pdf.
[367] Sudha Ramachandran, "India goes to war in space," *Asia Times*, June 18, 2008, http://www.atimes.com/atimes/South_Asia/JF18Df01.html.

capabilities to monitor India's disputed borders.[368] In July 2017, at a unified commanders' meeting conference, the defense secretary "apprised the audience that the Defence Cyber & Space Agencies and Special Operations Division will soon become a reality."[369] It is unclear what shape it will take.

Potential Military Utility

India reportedly earned 230 crore (or $36 million) by launching foreign satellites from 2015-2016.[370] India has been using satellite technologies for strategic purposes: reconnaissance, communications, and navigations. As of the fall of 2017, according to the Union of Concerned Satellites' Satellite Database, India had 50 active satellites.[371] The first satellite created specifically for the military was the GSAT-7 communications satellite, launched in August 2013.[372] It was designed and developed by ISRO, with the intent of being used by the Navy for communications and ELINT purposes. It was followed by GSAT-6, launched in August 2015, and again developed by ISRO for military communications purposes.[373] With the June 2017 launch of the Cartsat 2E+ Earth observation satellite, it was reported that India now has 13 satellites that are being used for military purposes.[374] India's answer to GPS – the Navigation with Indian Constellation (NAVIC) precision, navigation, and timing system - started off life as the Indian Regional Navigation Satellite System. It is a seven-satellite constellation that is intended to provide accuracy of 20 meters within India and within 1,500-2,000 km surrounding it.[375]

India has invested heavily in its national security space infrastructure and capabilities and incorporating those capabilities into its military operations; furthermore, it is receiving an increasing amount of income from launching satellites for other countries. While it is possible that Indian officials would decide to test an ASAT in order to be considered to be a space weapons state (in the parlance of the NPT), this capability is strictly theoretical and thus more likely to be useful as a bargaining chip or a way to demonstrate that India is keeping pace with China.

.

[368] Rajagopalan, "Need for an Indian Military Space Policy," pp. 206-207.
369 Saikat Datta, "The Indian military is once again trying to bring the three forces closer – but will it succeed?" *Scroll.in,* July 31, 2017, https://scroll.in/article/845332/the-indian-military-is-once-again-trying-to-bring-the-three-forces-closer-but-will-it-succeed.
370 Singh, "Isro's launch capability will get boost."
371 UCS Satellite Database, August 31, 2017, https://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database?ga=2.172973859.1830573647.1521059766-238948019.1518680330#.WqmI3OcpBPY.
372 Amit R. Saksena, "India and Space Defense," *The Diplomat*, March 22, 2014, http://thediplomat.com/2014/03/india-and-space-defense/.
373 Ajey Lele, "India's Strategic Space Programme: From Apprehensive Beginner to Ardent Operator," in *Space India 2.0: Commerce, Policy, Security and Governance Perspectives*, ed. Rajeswari Pillai Rajagopalan and Narayan Prasad (Observer Research Foundation, 2017), pp.190-191, http://cf.orfonline.org/wp-content/uploads/2017/02/ORF_Space-India-2.0.pdf.
374 Surendra Singh, "Military using 13 satellites to keep eye on foes," *Times of India*, June 26, 2017, http://timesofindia.indiatimes.com/india/military-using-13-satellites-to-keep-eye-on-foes/articleshow/59314610.cms.
[375] Lele, "India's Strategic Space Programme," p. 191.

7 – CYBER COUNTERSPACE CAPABILITIES

Assessment

Multiple counties likely possess cyber capabilities that could be used against space systems; however actual evidence of cyber attacks in the public domain are limited. The United States, Russia, China, North Korea, and Iran have all demonstrated the ability and willingness to engage in offensive cyber attacks against non-space targets. Additionally, a growing number of non-state actors are actively probing commercial satellite systems and discovering cyber vulnerabilities that are similar in nature to those found in non-space systems. This indicates that manufacturers and developers of space systems may not yet have reached the same level of cyber hardness as other sectors. But to date, there have only been a few publicly-disclosed cyber attacks directly targeting space systems.

There is a clear trend toward lower barriers to access, and widespread vulnerabilities coupled with reliance on relatively unsecured commercial space systems create the potential for non-state actors to carry out some counter-space cyber operations without nation-state assistance. However, while this threat deserves attention and will likely grow in severity over the next decade, there remains a stark difference at present between the cyber attacks capabilities of leading nation-states and other actors.

Specifics

Cyber capabilities include a broad set of different tools and techniques aimed at exploiting ever-changing vulnerabilities in each layer of the infrastructure that underpins space access. Extant capabilities have demonstrated the capacity to produce a wide range of strategic and tactical effects, both kinetic and non-kinetic. These include theft, alteration, or denial of information, as well as control or destruction of satellites, their subcomponents, or supporting infrastructure. As space capabilities continue to shift towards incorporating more advanced on-board processing, all-digital components, software-defined radios, packet-based protocols, and cloud-enabled high-performance computing, the attack surface for cyber attacks is likely to increase.

Cyber attacks against space capabilities are similar to cyber attacks against non-space systems. They often involve attempts to feed user-provided information to a system that causes software to perform in unexpected ways, commonly known as ”bugs”. In some cases, bugs can be exploited to crash systems, run unauthorized code, and/or gain unauthorized access. Other common cyber attacks exploit the lack of, or faulty, authentication of users and commands. The more software features or components a system has, and the more types and channels of data it processes, the higher the attack surface of potential vulnerabilities that an attacker can exploit. There is also an

unclear distinction between cyber attacks and electronic warfare, with some arguing for a merger of the two fields.[376]

Any cyber attack requires four things: access, vulnerability, a malicious payload, and a command-and-control system.[377] Three primary points of access exist for exploitation, attack, and service denial of space assets in the cyber domain: the supply chain, the extended land-based infrastructure that sustains space-based assets—including ground stations, terminals, related companies, and end-users—and the satellites themselves.[378] Successful penetration of any one of these may be sufficient to produce the desired espionage, 'soft'-, or 'hard'-kill effects, and also enables the launching of additional follow-on cyberattacks in other vectors.[379] A wide and rapidly growing array of tools and techniques threaten each of these levels.

As a result, cyber capabilities are critically important to the overall counter-space environment.[380] One former senior military official has gone so far as to identify cyber vulnerabilities as the "No. 1 counter-space threat," further underscoring their strategic significance. All major players appear extremely likely to continue the development and use of such capabilities.[381] In 2017, the U.S. Intelligence Community testified in its annual report before the Senate Select Committee on Intelligence that both Russia and China, driven by a perceived need to offset U.S. military

---

[376] Eric Chabrow, "Aligning Electronic and Cyber Warfare," *Gov Info Security*, July 10, 2012, https://www.govinfosecurity.com/aligning-electronic-cyber-warfare-a-4930.

[377] Andrea Gini, "Cyber Crime – From Cyber Space to Outer Space," *Space Safety Magazine*, February 14, 2014, http://www.spacesafetymagazine.com/aerospace-engineering/cyber-security/cyber-crime-cyber-space-outer-space/.

[378] Mark Holmes, "Cybersecurity Expert Assesses Potential Threats to Satellites," *Via Satellite*, February 21, 2017, http://www.satellitetoday.com/technology/2017/02/21/cybersecurity-expert-assess-potential-threats-satellites/; David Livingstone and Patricia Lewis, "Space, the Final Frontier for Cybersecurity?," Chatham House research paper https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf; Madeline Moon (Rapporteur), "The Space Domain and Allied Defence," NATO Parliamentary Assembly, Defence and Security Committee, Sub-Committee on Future Security and Defence Capabilities, October 8, 2017, https://www.nato-pa.int/download-file?filename=sites/default/files/2017-11/2017%20-%20162%20DSCFC%2017%20E%20rev%201%20fin%20-%20SPACE%20-%20MOON%20REPORT.pdf

[379] Eric Sterner and Jennifer McArdle, "Cyber Threats in the Space Domain," The American Foreign Policy Council, *Defense Technology Program Brief*, March 31, 2016, http://www.afpc.org/publication_listings/viewPolicyPaper/3149%20/true; Mark Holmes, "Cybersecurity Expert Assesses Potential Threats to Satellites," *Via Satellite*, February 21, 2017, http://www.satellitetoday.com/technology/2017/02/21/cybersecurity-expert-assess-potential-threats-satellites/; Jason D. Wood, "Strategic Security: Toward an Integrated Nuclear, Space, and Cyber Policy Framework," accessed March 23, 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/110916_Wood.pdf

[380] "Significant Security Deficiencies in NOAA's Information Systems Creates Risks in its National Critical Mission," National Oceanic and Atmospheric Administration, July 15, 2014, https://www.oig.doc.gov/OIGPublications/OIG-14-025-A.pdf; Mark Clayton, "Can military's satellite links be hacked? Cyber-security firm cites concerns.," *Christian Science Monitor*, April 25, 2014, https://www.csmonitor.com/World/Passcode/2014/0425/Can-military-s-satellite-links-be-hacked-Cyber-security-firm-cites-concerns; David Livingstone, "Cyberattacks in Space: We Must Defend the Final Frontier," *Newsweek*, November 26, 2014, http://www.newsweek.com/cyberattacks-space-we-must-defend-final-frontier-287525; David Livingstone and Patricia Lewis, "Space, the Final Frontier for Cybersecurity?," Chatham House research paper https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf; http://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/#gref.

[381] Kevin Pollpeter, "Testimony Before the U.S.-China Economic and Security Review Commission: Hearing on China's Advanced Weapons," *CNA*, February 2017, https://www.cna.org/CNA_files/PDF/CPP-2017-U-014906-Final.pdf.; Daniel Coats, "Statement for the Record – Worldwide Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence, February 13, 2018, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

advantages, are certain to continue to pursue a "full range" of counter-space capabilities.[382] Moreover, integration and complementary use of an array of ASAT capabilities—and particularly an increased "blending of EW and cyber-attack" capabilities—is likely to occur, representing a growing sophistication in tools and techniques for the denial and degradation of C4ISR networks.[383]

Categories of Cyber Attacks on Space Systems

Parsing the exact nature and extent cyber capabilities or development efforts with any precision based on the open source is a fraught exercise. There have been only a few cases of publicly-acknowledged cyber attacks against satellites, and even the information on those is incomplete. And cyber weapon development is one of the most sensitive and closely-guarded secrets kept by nation states. Still, some general conclusions may be drawn about the capabilities in existence based on a technical assessment of vulnerabilities and a review of known instances of use.

First, the risks to global supply chain security posed by the increasing use of faulty or counterfeit microelectronics and materials produced abroad have been well-documented.[384] Deliberate installation of hidden back doors in hardware or software products is another primary threat vector. Such back doors have been found in Chinese electronics[385] and Russian software packages[386] used by U.S. aerospace companies. The United States, meanwhile, has engaged in a broad and persistent campaign of computer network exploitation (CNE) operations for decades, with targets including

[382] Daniel Coats, "Statement for the Record – Worldwide Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence, May 11, 2017, https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf

[383] Ibid; see also Pollpeter,"Testimony Before the U.S.-China Economic and Security Review Commission: Hearing on China's Advanced Weapons."

[384] These are largely beyond the scope of this assessment. For a brief discussion of such efforts as part of broader counterspace programs, see James Clapper, "Statement for the Record – Worldwide Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence," February 26, 2015, https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf. For a useful taxonomy of supply chain attacks, refer to John Miller, "Supply Chain Attack Framework and Attack Patterns," *The MITRE Corporation*, December 2013, https://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf.

[385] One high-profile instance was the discovery by a Cambridge security researcher of a backdoor built into nonencrypted Microsemi chips utilized in a range of sensitive assets including weapons systems. Some experts alleged that this could be leveraged to attack and disable or destroy millions of systems. See Steven Musil, "Experts Dispute Threat Posed by Backdoor Found in Chinese Chip," *CNET*, May 29, 2012, https://www.cnet.com/news/experts-dispute-threat-posed-by-backdoor-found-in-chinese-chip/;Others disagreed, contending that the backdoor was either accidental or so difficult to exploit as to be largely irrelevant. See Robert Graham, "Bogus Story: No Chinese Backdoor in Military Chip," *Errata Security*, May 28, 2012, https://blog.erratasec.com/2012/05/bogus-story-no-chinese-backdoor-in.html.

[386] For example, Russia-based Kaspersky was used extensively by numerous governmental agencies, contractors, and private companies, and has been implicated in allowing Russia backdoor access to various networks including that of the U.S. National Security Agency (NSA). See Gordon Lubold and Shane Harris, "Russian Hackers Stole NSA Data on U.S. Cyber Defense," *The Wall Street Journal*, October 5, 2017, https://www.wsj.com/articles/russian-hackers-stole-nsa-data-on-u-s-cyber-defense-1507222108.

foreign telecommunications and aerospace infrastructure.[387] There have also been media reports of U.S. intelligence agencies intercepting shipments of commercial equipment to install "implants"[388], and creating backdoors in commercial encryption software.[389] Similar cyber-espionage operations can be directed against satellite manufacturers, parts suppliers, software brokers, launch service providers, and telecommunications companies are also common. Physical infiltration, social engineering, and network exploitation of these targets can provide access to the design schematics, physical components, and software packages of a given satellite.

The second category of cyber attacks are those directed against the links between satellites and ground control stations. Most of these are likely to be man-in-the-middle (MITM) attacks, an umbrella term that involves an attacker inserting themselves between the sender and receiver, thus able to monitor information being passed or perhaps even modify it. It is also possible - although often very difficult—to use a cyber attack against the command and control (C2) link to gain access to the satellite bus or payloads. This type of attack is made easier if the C2 system is unencrypted or does not properly authenticate commands. If such an attack is successful, there is little limit to the damage that can be done.

Over the last decade, there have been a few public examples of satellite C2 links being attacked (or alleged instances of attacks). In 2007, it was reported that the Tamil Tigers extremist separatist group successfully hacked ground C2 nodes and gained control of the broadcasting capabilities of a U.S. commercial satellite.[390] From 2007 through 2009, there were multiple incidents of attacks against C2 links for NASA satellites that are thought to be attributed to China, as detailed in the 2011 report of the U.S.-China Economic and Security Review Commission.[391] In October 2007, the Landsat 7 remote sensing satellite experienced twelve minutes of interference, . In June of 2008, the Terra EOS AM-1 remote sensing satellite experienced two minutes of interference, and the attackers achieved "all steps required to send commands but did not." On July 23, 2008, Landsat experienced another twelve minutes of interference, but the attackers did not gain access to the C2 link. But on October 22, 2008, the Terra satellite experienced another nine minutes of interference, and once again the attackers gained control of the satellite but did not exercise it.

---

[387] Of particular note are the operations of the Office of Tailored Access Operations (TAO) in the NSA, housed jointly with U.S. Cyber Command (Cybercom) at Fort Meade. The TAO has consistently and comprehensively penetrated foreign computer and telecommunications systems, through an ever-evolving range of methods including the installation of physical backdoors in Chinese components or systems at various stages of production, distribution, and use to ensure remote access. See Matthew Aid, "Inside the NSA's Ultra-Secret China Hacking Group," *Foreign Policy*, June 10, 2013, http://www.foreignpolicy.com/articles/2013/06/10/inside_the_nsa_s_ultra_secret_china_hacking_group; "Documents Reveal Top NSA Hacking Unit," *Der Spiegel*, December 29, 2013, http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html.

[388] Sean Gallagher, "Photos of an NSA'Upgrade' Factory Show Cisco Router Getting Implant," *Arstechnica*, May 14, 2014, https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/

[389] Joseph Menn, "Exclusive: Secret Contract Tied NSA and Security Industry Pioneer," *Reuters*, December 20, 2013, https://www.reuters.com/article/us-usa-security-rsa/exclusive-secret-contract-tied-nsa-and-security-industry-pioneer-idUSBRE9BJ1C220131220.

[390] Jill Stuart, "Comment: Satellite Industry Must Invest in Cyber Security," *The Financial Times*, April 10, 2015, https://www.ft.com/content/659ab77e-c276-11e4-ad89-00144feab7de.

[391] "2011 Report to Congress of the U.S.-China Economic and Security Review Commission," *U.S. Economic and Security Review Commission*, November 2011, p. 216, https://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf.

Initial reports traced events to the Kongsberg Satellite Services ground station at Svalbard, but they said their systems could not command NASA satellites.[392] General Robert Kehler, then commander of United States Strategic Command, said there was no evidence to attribute the attacks at the time.[393]

The third category involves attacks on terrestrial C2 or data relay stations. Techniques could include fly-overs with manned aircraft, unmanned aerial systems (UAS), or weather balloons;[394] signal disruption or hijacking through proximate positioning of broadcasting equipment using a more powerful signal, tapping the structure's Internet or Ethernet cables, or piggybacking off of the station's own data relays;[395] physical access, through either covert infiltration or social engineering;[396] and network exploitation or attack, using traditional means.[397] Although many satellite C2 facilities are hardened against cyber attacks and take precautions such as "air-gapping" critical networks, there are examples of sophisticated State attackers being able to penetrate such systems.[398]

Also in this third category are cyber attacks against ground systems that process space data. NASA, for example, has long been the target of cyberattacks, as have other space agencies around the world.[399] In late 2014, attackers breached NOAA's computer network, including systems used to manage and disseminate satellite weather data and products includes the National Environmental Satellite, Data, and Information Service and the National Earth System Prediction Capability.[400] Although the attack itself did not disrupt satellite data, NOAA stopped providing satellite imagers to the National Weather Service and public-facing services were taken offline for two days while

---

[392] Jim Wolf, "China Key Suspect in U.S. Satellite Hacks; Commission," *Reuters*, October 28, 2011, https://www.reuters.com/article/us-china-usa-satellite/china-key-suspect-in-u-s-satellite-hacks-commission-idUSTRE79R4O320111028.

[393] Ibid.

[394] This allows easy access for signal interference or hijacking. See Andy Greenberg, "How to Hack the Sky," *Forbes*, February 2, 2010, https://www.forbes.com/2010/02/02/hackers-cybercrime-cryptography-technology-security-satellite.html#2153b10f731f; Andrea Gini, "Cybercrime – From Cyber Space to Outer Space," *Space Safety Magazine*, February 14, 2014, http://www.spacesafetymagazine.com/aerospace-engineering/cyber-security/cyber-crime-cyber-space-outer-space/

[395] Rajeswari Pillai Rajagopalan and Daniel Porras, "Cyber Arms Race in Space: Exploring India's Next Steps," *Observer Research Foundation Issue Brief*, Issue No. 113, November 2015, http://www.orfonline.org/wp-content/uploads/2015/12/Issue-Brief_113.pdf; Juliet Van Wagenen, "WTA Urges Teleport Operators to Improve on Cybersecurity," *Via Satellite*, August 5, 2015, http://www.satellitetoday.com/innovation/2015/08/05/wta-urges-teleport-operators-to-improve-on-cyber-security/.

[396] Ibid.

[397] Ibid; this approach has been taken by China in particular, see: Robert Lai and Syed Rahman, "Analytic of China Cyberattack," *The International Journal of Multimedia and Its Applications*, Vol 4 No 3, June 2012, https://www.researchgate.net/publication/267363551_Analytic_of_China_Cyberattack.

[398] David Kushner, "The Real Story of Stuxnet," *IEEE Spectrum Magazine*, February 26, 2013, https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

[399] Paul Martin, "NASA Cybersecurity: An Examination of the Agency's Information Security," testimony before the House Subcommittee on Investigations and Oversight, February 29, 2012, https://oig.nasa.gov/congressional/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf; Nafeesa Syeed, "Outer-Space Hacking a Top Concern for NASA's Cybersecurity Chief," *Bloomberg*, April 12, 2017, https://www.bloomberg.com/news/articles/2017-04-12/outer-space-hacking-a-top-concern-for-nasa-s-cybersecurity-chief.

[400] 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?utm_term=.d01b2f4051a7

the systems were cleaned. While the U.S. government did not publicly attribute the attack, Rep. Frank Wolf declared that "NOAA told me it was a hack and it was China."[401]

A fourth category involves cyber attacks against the user segment of a space system, often the terminals or devices used to receive or process a satellite signal. In many cases, these attacks are very similar to cyber attacks against other types of computer equipment and focus on exploiting hardware or software vulnerabilities in the devices. As an example, a group of American university students developed a technique for attacking the software in common commercial GPS receivers.[402] The attack uses a specially-built box that modifies the data content of real civil GPS signals, and rebroadcast them. When a GPS receiver tries to decode these malicious GPS signals, they can crash or go into constant reboot loops, effectively succumbing to a denial-of-service attack. Another report in 2014 found that over 10,000 allegedly-secure very small aperture terminals (VSATs) used for transmission of critical information—including classified defense-relevant communications, sensitive financial data, and supervisory control and data acquisition (SCADA) system data essential to the continued operation of power grids and oil rigs in the United States—were easily scanned and penetrated from abroad due to a simple failure to change default factory password settings or disable outward-facing virtual network (telnet) access.[403]

Iridium, a satellite communications company whose single largest client is the Pentagon, provides another example of commercial satellite systems being behind other sectors in cyber hardening. In 2008, Iridium reportedly boasted that "the complexity of the Iridium air interface makes the challenge of developing an Iridium L-Band monitoring device very difficult and probably beyond the reach of all but the most determined adversaries".[404] A group of hackers promptly determined that it was possible to effectively eavesdrop on Iridium traffic with nothing more than a cheap, easily-accessible software-defined radio and the processing power of an old, low-end laptop.[405] While development and launch of next-generation satellite networks including Iridium NEXT should assist somewhat, this highlights the severity of the threat posed by reliance on legacy infrastructure, and the insecurity of satellite architectures generally. Other techniques, including the use of ransomware in embedded space and aerospace systems and the transmission of

[401] Ibid; Timothy Cama, "Report: Chinese Hacked U.S. Weather Systems," *The Hill*, November 12, 2014, http://thehill.com/policy/energy-environment/223871-report-chinese-hacked-us-weather-systems.
[402] Tyler Nighswander et al, "GPS Software Attacks", *Carnegie Mellon University*, 2012, https://users.ece.cmu.edu/~dbrumley/pdf/Nighswander%20et%20al._2012_GPS%20software%20attacks.pdf.
[403] Office of Inspector General, "Significant Security Deficiencies in NOAA's Information Systems Create Risks in Its National Critical Mission," *U.S. Department of Commerce*, July 15, 2014, https://www.oig.doc.gov/OIGPublications/OIG-14-025-A.pdf; Ruben Santamarta, "A Wake-Up Call for SATCOM Security," *IOActive*, 2014, https://www.ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf; Bonnie Zhu, Anthony Joseph, and Shankar Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems," *Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, October 19-22, 2011, http://bnrg.cs.berkeley.edu/~adj/publications/paper-files/ZhuJosephSastry_SCADA_Attack_Taxonomy_FinalV.pdf; Darlene Storm, "Hackers Exploit SCADA Holes to Take Full Control of Critical Infrastructure," *ComputerWorld*, January 15, 2014, https://www.computerworld.com/article/2475789/cybercrime-hacking/hackers-exploit-scada-holes-to-take-full-control-of-critical-infrastructure.html
[404] 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.
[405] Ibid.

malicious code from compromised ground stations, have also begun to emerge, with one large-scale 2016 attack costing a mere estimated $1,000 worth of hardware to execute, albeit with a substantial investment in time and effort.[406] Even modern platforms with a "high degree of security" engineered-in are vulnerable to such attacks due to the degree to which they necessarily rely upon and interact with highly vulnerable legacy and civilian systems.[407]

In 2014, Crowdstrike released a report tracing the activities of an advanced persistent threat (APT), based in Shanghai and affiliated with the PLA General Staff Department Third Department 12th Bureau Unit 61486—that subset of what is "generally acknowledged to be China's premier SIGINT collection and analysis agency" dedicated specifically to "supporting China's space surveillance network" with a "functional mission involving satellites...inclusive of intercept of satellite communications."[408] Dubbed "Putter Panda," the group was found to have conducted comprehensive and sustained penetration and cyber-espionage operations targeted at the U.S. defense and European satellite and aerospace industries since at least 2007.[409] This included, among other things, the use of Remote Access Tools (RATs) on space technology targets, controlled from the physical location of the 12th Bureau's headquarters. This toolset, the report notes, "provide[d] a wide degree of control over a victim system and can provide the opportunity to deploy additional tools at will."[410]

A related category, not strictly "counterspace" but nevertheless an important consideration in the context of cyberattacks on space assets, is the exploitation of satellite links to facilitate hacking of other targets. This recently made headlines when Kaspersky Labs discovered that Russian criminal syndicate Turla had been doing so to great effect since at least 2007.[411] Turla's technique, which couples a compromised PC using satellite-based Internet with a MITM attack, hijacks the IP addresses of legitimate users. This approach allows the hacker to anonymize Internet connections, impersonate legitimate high-speed Internet users, spoof DNS requests, and gain access to private networks.[412] When used as an anonymizer for subsequent attacks against high-value targets, this approach makes it very difficult to network analysts and law enforcement agencies to correctly attribute operations, or to locate and disable command servers.[413] Perhaps worst of all, information on these techniques is readily available in the public domain, and the steps are easily replicable by

---

[406] http://www.satellitetoday.com/technology/2017/02/21/cybersecurity-expert-assess-potential-threats-satellites/
[407] Ruben Santamarta, "A Wake-Up Call for SATCOM Security"; Office of Inspector General, "Significant Security Deficiencies in NOAA's Information Systems Create Risks in Its National Critical Mission,". For more on penetration of ground stations and upstream communications networks, see also Kazuto Suzuki, "Satellites, the Floating Targets," *The World Today*, February and March 2016, pp 15-16, https://www.chathamhouse.org/system/files/publications/twt/Satellites,%20the%20floating%20targets.pdf
[408] CrowdStrike Intelligence Report: Putter Panda," *CrowdStrike*, June 9, 2014, https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf.
[409] Ibid.
[410] Ibid.
[411] Stefan Tanase, "Satellite Turla: APT Command and Control in the Sky," *SecureList*, September 9, 2015, https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/.
[412] Ibid.
[413] Ibid; Kim Zetter, "Russian Spy Gang Hijacks Satellite Links to Steal Data," *Wired*, September 9, 2015, https://www.wired.com/2015/09/turla-russian-espionage-gang-hijacks-satellite-connections-to-steal-data/.

any motivated attacker with an intermediate skill level. Notably, the necessary tools (a low-budget satellite receiver card, open source Linux applications, and widely-available network sniffing tools) cost only around $75 in total.[414] A more sophisticated version of the technique that is harder to detect, differentiate, and counter can be achieved with only a satellite dish, cheap cables, and a satellite modem—a total cost of roughly $1,000.[415] The downsides of this approach are that satellite-based Internet is slow, and access through a hijacked account is unreliable and user-dependent. The benefits to an attacker seeking to carry out a sustained campaign with little risk of detection or successful attribution, however, are enormous.[416]

Most leading subject matter experts maintain that across each of these areas, despite some increase in awareness of the threat in recent years, the state of cybersecurity for satellite infrastructure remains dismal.[417] This, in turn, provides both state and non-state actors with a back door into a wide array of space- and ground-based critical infrastructures.

While little information is publicly available regarding other Russian cyberattacks targeted at space assets, Russia has demonstrated significant cyber attack capabilities in a range of other contexts, as well as the willingness to use them. In one of the few publicly known attacks against a satellite, in 1998 hackers based in Russia hijacked control of a U.S.-German ROSAT deep-space monitoring satellite, then issued commands for it to rotate toward the sun, frying its optics and rendering it useless.[418] More recently since the end of 2015, Russia has engaged in a coordinated, escalating cyber attack campaign in recent conflicts in Georgia and Ukraine that ranges from prolonged low-level cyber-espionage, sabotage, and information warfare to the use of offensive cyber operations with kinetic effects.[419] Most notably, this campaign included the physical incapacitation of Ukrainian power grids.[420] Cyber experts believe that, while the damage was limited and the resultant outages temporary, this was the result of deliberate restraint on the part of Russia for signaling purposes, and that the sophistication of the cyberattack and degree of access

[414] One amateur hacker's presentation at a BlackHat conference in 2010 is illustrative: Leonard Nve Egea, "Playing in a Satellite Environment 1.2," *Black Hat*, August 2010, http://www.blackhat.com/presentations/bh-dc-10/Nve_Leonardo/BlackHat-DC-2010-Nve-Playing-with-SAT-1.2-wp.pdf.
[415] Kim Zetter, "Russian Spy Gang Hijacks Satellite Links to Steal Data," *Wired*, September 9, 2015, https://www.wired.com/2015/09/turla-russian-espionage-gang-hijacks-satellite-connections-to-steal-data/
[416] Ibid.
[417] David Livingstone and Patricia Lewis, "Space, the Final Frontier for Cybersecurity?", *Chatham House*, September 2016, https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf.
[418] Ben Elgin, "Network Security Breaches Plague NASA," *Bloomberg*, November 20, 2008, https://www.bloomberg.com/news/articles/2008-11-19/network-security-breaches-plague-nasa; Jason Fritz, "Satellite Hacking: A Guide for the Perplexed," *The Bulletin of the Centre for East-West Cultural and Economic Studies*, Vol 10 Issue 1, Article 3, 2013, http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1131&context=cm.
[419] Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," *CNA*, March 2017, https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf; Azhar Unwal and Shaheen Ghori, "Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict," *Military Cyber Affairs*, Vol 1 Issue 1, Article 7, 2015, http://scholarcommons.usf.edu/mca/vol1/iss1/7/.
[420] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

achieved would have allowed the attackers to inflict extensive physical damage and bring the power stations permanently offline had they wished to do so.[421]

These examples have caused significant concern in other countries, including the United States. Since at least March 2016, for example, Russian governmental actors have carried out a systematic and wide-ranging cyber offensive targeted at key U.S. government agencies and critical infrastructure sectors. A joint report released in March 2018 by the Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI), and supplemented by threat intelligence from cybersecurity firms including Symantec, chronicled penetration and exploitation of computer networks and Industrial Control Systems (ICS) across the nuclear, water, defense, aviation, critical manufacturing, and energy sectors, among others.[422] Of particular note is the highly-sophisticated character of these attacks, which appear to have deliberately chosen hard but strategically vital targets and tested a flexible and advanced array of tools and techniques, deployed as part of a two-step operation in which access would first be gained to less-secure "staging targets", whose networks were then used as additional attack vectors and malware repositories.[423] Given these examples and many others, there is no reason to believe that Russia is incapable of conducting similar operations in the space domain.

While there is no public evidence of government-sponsored Iranian cyber attacks directly targeted at space assets, Iranian cyber capabilities have exhibited steady growth in recent years. By the mid-2000s, a range of Islamic Revolutionary Guard Corps (IRGC)-backed Iranian hacktivist organizations had begun carrying out computer network attack and exploitation operations against other nation-states. These escalated steadily over the ensuing decade: by 2012, Iranian hackers were conducting cyberattacks with kinetic effects against Saudi oil and gas infrastructure and engaging in sustained distributed denial-of-service (DDOS) campaigns against major U.S. banks causing tens of millions of dollars in losses.[424] In 2013, hackers with apparent ties to the IRGC successfully penetrated critical infrastructure in the United States, temporarily gaining control over a dam in the New York suburbs.[425] In late 2016 and early 2017, Iranian hackers engaged in a comprehensive cyber-espionage campaign aimed at identifying and gaining leverage over certain outgoing and incoming American officials, particularly those affiliated with the State

[421] Ibid; "Analysis of the Cyber Attack on the Ukrainian Power Grid," *SANS Industrial Control Systems*, March 18, 2016, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.
[422] "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," *US-CERT*, March 15, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A; "Dragonfly: Western Energy Sector Targeted By Sophisticated Attack Group," *Symantec Corporation*, October 20, 2017, https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks.
[423] "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," *US-CERT*, March 15, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A.
[424] Dorothy Denning, "Iran's Cyber Warfare Program is Now A Major Threat to the United States," *Newsweek*, December 12, 2017, http://www.newsweek.com/irans-cyber-warfare-program-now-major-threat-united-states-745427.
[425] Mark Thompson, "Iranian Cyber Attack on New York Dam Shows Future of War," *Time*, March 24, 2016, http://time.com/4270728/iran-cyber-attack-dam-fbi/; Evan Perez and Shimon Prokupecz, "First on CNN: U.S. Plans to Publicly Blame Iran for Dam Cyber Breach," *CNN*, March 10, 2016, https://www.cnn.com/2016/03/10/politics/iran-us-dam-cyber-attack/index.html.

Department.[426] During the same time period, Iranian cyberattacks against Saudi Arabia resulted in mass-deletion of data across "dozens" of networks, both government-owned and private.[427] In early 2018, cybersecurity firm Symantec announced that "Chafer," an Iran-based hacking group believed largely due to its choice of targets to be government-affiliated, had successfully penetrated a range of targets including defense contractors, aviation forms, a major Middle Eastern telecommunications provider, and a variety of networks in Israel, Jordan, the United Arab Emirates, Saudi Arabia, and Turkey, using both original tools and exploits previously stolen from the U.S. National Security Agency (NSA) in 2017 by a third party.[428] Given the consistent pattern of interest in and willingness to use offensive cyber capabilities, as well as the tactical and strategic context in which Iran finds itself,[429] eventual deployment of such capabilities against space-related infrastructure in at least limited ways appears highly likely, and may have already occurred.

North Korea's cyber capabilities appear to be even more sophisticated, and are likely to continue advancing rapidly, absent significant disruption on the Peninsula.[430] Particularly prominent examples of offensive cyber operations by North Korea-backed hackers include a highly-publicized 2014 hack of Sony Pictures Entertainment, intended to prevent the theatrical release of a film satirizing Kim Jong-un;[431] hacks of US and South Korean civilian critical infrastructure and military networks, with outcomes ranging from insertion of digital kill-switches intended to paralyze power supplies on-demand to successful theft of war plans;[432] WannaCry, a global ransomware attack in May 2017 which made use of existing North Korean capabilities supplemented by stolen NSA tools and demonstrated a capability to shut down large swathes of the economy and critical industries around the world;[433] and frequent and sustained cyber-espionage and cyber crime campaigns targeted at, among other things, large banks and financial

[426] For more on these attacks, as well as a comprehensive treatment of the past, present, motivations, and likely future of Iranian operations in cyberspace, refer to: "Iran's External Targets," *Carnegie Endowment for International Peace*, January 4, 2018, http://carnegieendowment.org/2018/01/04/iran-s-external-targets-pub-75141.
[427] Daniel Coats, "Statement for the Record – Worldwide Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence, February 13, 2018, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.
[428] Morgan Chalfant, "New Attacks Spark Concerns About Iranian Cyber Threat," *The Hill*, March 11, 2018, http://thehill.com/policy/cybersecurity/377672-new-attacks-spark-concerns-about-iranian-cyber-threat; Morgan Chalfant, "Iranian Hacking Group Appears to Expand International Operations," *The Hill*, February 28, 2018, http://thehill.com/policy/cybersecurity/376015-iranian-hacking-group-expands-operations-to-international-targets
[429] For more on this as it relates to the space context, see *Infra* ___
[430] David Sanger, David Kirkpatrick, and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More.," *The New York Times*, October 15, 2017, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html.
[431] Ibid.
[432] Ibid. It is worth noting that these operations are in no way one-sided: there is substantial evidence of similar operations by both the US and South Korean governments.
[433] Thomas Bossert, "It's Official: North Korea is Behind WannaCry," *The Wall Street Journal*, December 18, 2017, https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537; Ellen Nakashima and Phillip Rucker, "U.S. Declares North Korea Carried Out Massive WannaCry Cyberattack," *The Washington Post*, December 19, 2017, https://www.washingtonpost.com/world/national-security/us-set-to-declare-north-korea-carried-out-massive-wannacry-cyber-attack/2017/12/18/509deb1c-e446-11e7-a65d-1ac0fd7f097e_story.html; "Investigation: WannaCry Cyber Attack and the NHS," *National Audit Office*, October 27, 2017, https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

institutions,[434] cryptocurrency exchanges,[435] and defense and defense-adjacent companies.[436] Many of these capabilities, especially those highlighted in the WannaCry incident, could cause tremendous damage if targeted at terrestrial infrastructure supporting space operations. Other cyber tools and techniques with counter-space implications likely either already exist or will in the not-too-distant future.

Potential Military Utility

Cyber weapons offer tremendous utility as both a situational replacement for and complement to conventional counter-space capabilities. Several advantages are particularly noteworthy, although there are disadvantages as well.

The first advantage is the flexibility and nature of producible effects. Extant cyber and electronic warfare capabilities can produce a range of effects, including theft, alteration, or denial of information, as well as control or destruction of satellites, their subcomponents, or supporting infrastructure. This allows the type and degree of counter-space operation to be narrowly tailored to the desired objective, in contrast to the comparatively blunt and single-not instrument that a kinetic ASAT represents. No other capability can fulfill such an espionage or data manipulation role, while the ability to reliably produce kinetic outcomes of the desired severity and permanence holds obvious appeal.

The second advantage for cyber attacks in a counterspace role is access. Unlike conventional weapons which typically require either proximate positioning or closing to target, both of which necessarily involve penetration of defended space, some types of cyber attacks require little or no direct access, or can be effectuated by gaining access far in advance or targeting less closely-guarded nodes.[437]

The third advantage is the difficulty of attributing cyber attacks. Cyber attacks are often substantially more difficult to trace and confidently attribute than conventional counter-space weapons, particularly kinetic weapons. This can be valuable, but also carries some risk of unintended escalation. The military value of being able to carry out operations either undetected or in a deniable fashion is clear. However, many strategic theorists have noted the danger of quick

[434] David Sanger, David Kirkpatrick, and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More.," *The New York Times*, October 15, 2017, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html; Choe Sang-Hun, "North Korea Tries to Make Hacking a Profitable Center," *New York Times*, July 27, 2017, https://www.nytimes.com/2017/07/27/world/asia/north-korea-hacking-cybersecurity.html.
[435] Rosie Perper, "New Evidence Reportedly Puts North Korean Hackers Behind a List of High-Stakes Bitcoin Heists," *Business Insider*, January 19, 2018, http://www.businessinsider.com/north-korea-lazarus-group-behind-cryptocurrency-cyber-attack-wannacry-sony-2018-1.
[436] Joe Uchil, "North Korean Hackers Target U.S. Military Contractors," *The Hill*, August 15, 2017, http://thehill.com/policy/cybersecurity/346594-with-leaders-talking-nuclear-war-north-korean-hackers-target-us-military; Anthony Kasza, "The Blockbuster Saga Continues," *Palo Alto Networks*, August 14, 2017, https://researchcenter.paloaltonetworks.com/2017/08/unit42-blockbuster-saga-continues/.
[437] Eric Sterner and Jennifer McArdle, "Cyber Threats to the Space Domain," *The American Foreign Policy Council*, March 2016, http://www.afpc.org/publication_listings/viewPolicyPaper/3149%20/true.

escalation that such can attend such deliberately opaque approaches, as the difficulty of guaranteeing a reliable and proportional response can create structural incentives for each side to move first in the event of an impending crisis.[438] These dangers are magnified by the potential for misattribution, whether incidental or deliberately engineered by actors intending to provoke a hostile response against another state.

Fourth, a rudimentary cyber capability can be dramatically faster, easier, and less expensive to procure than kinetic alternatives. The barrier to entry for basic capabilities can be exceptionally low as evidenced by the increased number of hobbyists and students researching cyber vulnerabilities in space systems. Advanced capabilities remain challenging to develop but will almost certainly become easier for new nation-states and even non-state actors to acquire in coming years. In contrast, conventional counterspace operations require expensive, time-consuming, and highly-visible development of an extensive space program, including systems for space situational awareness and space tracking, telemetry, and command operations, as well as the counter-space capability itself and its supporting infrastructure.[439] Thus, cyber capabilities provide newcomers with an especially asymmetric means of access-denial or cost infliction when confronting established space powers.

The main disadvantages of cyber capabilities are similar to that of other non-kinetic counterspace methods: lack of ability to do strategic signaling, and challenges in doing battle damage assessment. The inherent challenges in attributing cyber capabilities also have the effect of making it difficult to use the existence or use of offensive cyber counterspace for deterrence, signaling intent, or preventing escalation. And it can also be difficult for an attacker to know if their cyber attack will succeed, particularly in a militarily-useful timeframe, and if it will have the desired effect. It is always possible that the target has detected the preparations, or patched the vulnerability, and may even be able to deceive the attacker into thinking the attack worked, thus potentially undermining the broader military campaign it supported.

A final thing of note is the potential for joint "combined arms" anti-satellite operations, leveraging ASAT interoperability to produce a multiplier effect on the scale and effectiveness of counter-space operations.[440] This approach seeks to leverage cyber capabilities in ways complementary to physical ASATs and vice-versa--by, for example, using co-orbital KKVs as a delivery vehicle for EW capabilities, or using pre-installed back doors to deactivate sensors or countermeasures in advance of a kinetic operation. China and Russia, in particular, have explored such an idea from

[438] Todd Harrison et al, "Escalation and Deterrence in the Second Space Age," *Center for Security and International Studies*, October 2017, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/171017_Harrison_EscalationDeterrenceSecondSpaceAge_Web.pdf.
[439] For example, even the most rudimentary KKV capability requires a comprehensive, reliable, and ideally relatively rapid and resilient launch infrastructure, launch vehicles, rocket engines, onboard sensors and guidance systems, and a warhead or highly-maneuverable satellite.
[440] "China's Advanced Weapons," *Hearing Before the U.S.-China Economic and Security Review Commission*, February 23, 2017, https://www.uscc.gov/sites/default/files/transcripts/China%27s%20Advanced%20Weapons.pdf.

both the technical and doctrinal sides, and there is clear evidence of interest and significant evidence pointing to actual development on the part of the former.[441]

[441] Kevin Pollpeter et al, "China Dream, Space Dream: China's Progress in Space Technologies and Implications for the United States," *U.S.-China Economic and Security Review Commission*, March 2, 2015, https://www.uscc.gov/sites/default/files/Research/China%20Dream%20Space%20Dream_Report.pdf; "China's Advanced Weapons," *Hearing Before the U.S.-China Economic and Security Review Commission*, February 23, 2017, https://www.uscc.gov/sites/default/files/transcripts/China%27s%20Advanced%20Weapons.pdf; Daniel Coats, "Statement for the Record Worldwide Threat Assessment of the U.S. Intelligence Community - Senate Select Committee on Intelligence," *Office of the Director of National Intelligence*, May 11, 2017, https://www.intelligence.senate.gov/sites/default/files/documents/os-coats-051117.pdf.

8 – APPENDIX: IMAGERY OF MAJOR TEST SITES AND FACILITIES

Launch Complexes

China

Jiuquan

Function:	**Associated Programs:**
Space launch center and missile test complex	DN-2, DN-3, SC-19
Coordinates:	**Key Dates:**
41.281777 N 100.306390 E (ASAT/ABM target launch site)	January 11, 2010 (target launch supporting SC-19 launch from Korla) January 20, 2013 (target launch supporting SC-19 launch from Korla) July 23, 2014 (target launch supporting DN-2 or SC-19 launch from Korla) October 31, 2015 (possible target launch supporting DN-3 launch from Korla) December 9, 2016 (possible target launch supporting DN-3 launch from Korla, July 23, 2017 (possible target launch supporting DN-3 launch from Korla)

Figure 14 - Jiuquan

A launch complex at the Jiuquan Space Launch Center is used for testing mobile ballistic missiles. The above image shows a probable TEL possibly intended to launch the target for the December 9, 2016 DN-3 ASAT launch from Korla West.

Korla West

Function:	**Associated Programs:**
Missile test complex	DN-2, DN-3, SC-19
Coordinates:	**Key Dates:**
41.537300 N 86.353317 E (garrison complex) 41.537667 N 86.372073 E (ABM/ASAT launch pad)	January 11, 2010 (SC-19 ASAT test) January 20, 2013 (SC-19 ASAT test) July 23, 2014 (DN-2 or SC-19 ASAT test) October 31, 2015 (DN-3 ASAT test) December 9, 2016 (DN-3 ASAT test) July 23, 2017 (DN-3 ASAT test)

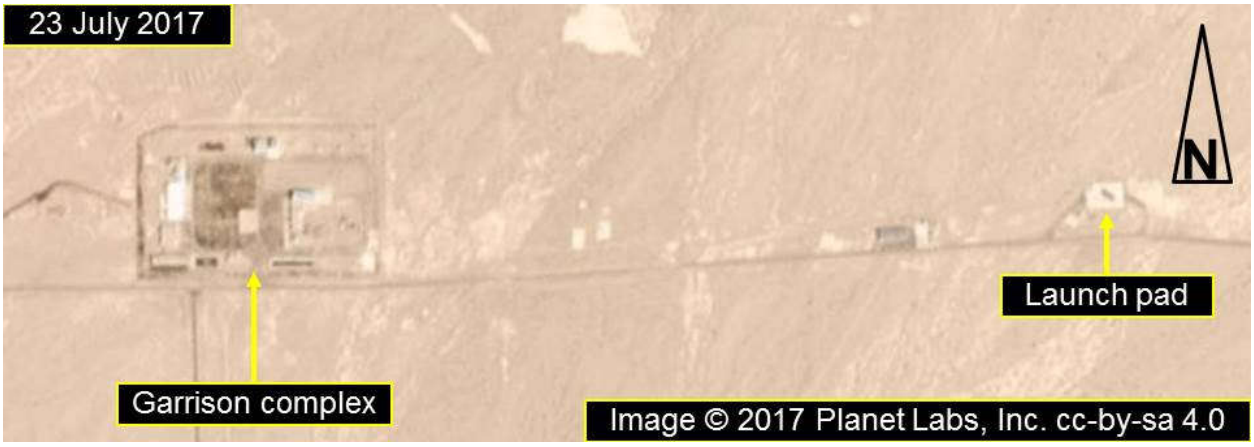

Figure 15 - Korla 1

The Korla West test complex is used for testing various ASAT and ABM/ATBM systems. A garrison complex serves the facility, with ASAT launches occurring from a launch pad to the east.

Figure 16 - Korla 2

The ASAT launch pad at Korla West employs a relocatable shelter for TEL concealment. The above image shows the TEL shelter placed on the launch pad for the July 23, 2017 DN-3 test.

Figure 17 - Korla 3

By August 7, 2017, the relocatable TEL shelter was displaced to the edge of the launch pad, following the July 23, 2017 DN-3 test.

Taiyuan

Function:	**Associated Programs:**
Space launch center and missile test complex	DN-3
Coordinates:	**Key Dates:**
38.840519 N 111.604648 E (possible ASAT/ABM target launch site) 38.836772 N 111.605964 E (possible ASAT/ABM target launch site)	December 9, 2016 (possible target launch supporting DN-3 launch from Korla, possible target TEL sighted on November 23, 2016) July 23, 2017 (possible target launch supporting DN-3 launch from Korla, possible target TEL sighted on July 19, 2017)

Figure 18 - Taiyuan

Taiyuan Space Launch Center possesses multiple launch pads serving mobile missile development. The northern pad, constructed between 2012 and 2013, possesses a TEL shelter translating on rails for launches. Of the southern pads, the northernmost example possesses a large relocatable shelter for concealing ICBM-sized TELs. The TEL shelter is large enough to permit erecting of the missile tube under cover. The above image captured on July 19, 2017 shows a possible TEL within the shelter, potentially serving as a target for the July 23, 2017 DN-3 test from Korla West.

Xichang

Function:	**Associated Programs:**
Space launch center and missile test complex	DN-2, SC-19
Coordinates:	**Key Dates:**
28.249140 N 102.022942 E (northern ABM/ASAT and target launch pad) 28.242775 N 102.032946 E (southern ABM/ASAT and target launch pad)	July 5, 2005 (SC-19 ASAT test) February 6, 2006 (SC-19 ASAT test) January 11, 2007 (SC-19 ASAT test) May 13, 2013 (DN-2 ASAT test)

Figure 19 - Xichang

Xichang Space Launch Center possesses launch pads at the northwest and southeast end of the facility possibly supporting SC-19 and DN-2 ASAT tests. Imagery captured on April 3, 2013 showed a DN-2 ASAT TEL on the southeastern pad prior to the May 13, 2013 test. The northwestern pad gained a relocatable shelter in 2016 similar to that seen at Korla West, suggesting that additional ASAT or ABM/ATBM related testing will resume at the location.

Russia

Kapustin Yar

Function:	**Associated Programs:**
Missile test and training complex	Nudol
Coordinates:	**Key Dates:**
48.794055 N 45.734890 E (SAM test complex) 48.662984 N 45.685747 E (SAM checkout complex) 48.569969 N 45.903070 E (ballistic missile test complex) 48.770544 N 46.303367 E (missile test complex)	December 16, 2016 (possible Nudol ASAT test)

Figure 20 - Kapustin Yar

The mobile missile training and launch area at Kapustin Yar is a possible location for the December 16, 2016 Nudol ASAT test.

Plesetsk

Function:	**Associated Programs:**
Space launch center and missile test complex	Nudol
Coordinates:	**Key Dates:**
63.008092 N 41.551308 E (mobile missile launch complex)	August 12,2014 (Nudol ASAT test) April 22, 2015 (Nudol ASAT test) November 18, 2015 (Nudol ASAT test) May 25, 2016 (Nudol ASAT test)

Figure 21 - Plesetsk

The Plesetsk mobile missile launch complex consists of a TEL garage with a retractable roof for conducting mobile ICBM launches and a separate launch pad. Either location represents a possible site for the Nudol ASAT tests conducted at Plesetsk.

Sary Shagan

Function:	**Associated Programs:**
SAM and ABM test complex	51T6, 53T6, 53T6M
Coordinates:	**Key Dates:**
46.443219 N 72.849398 E (Site 35 ABM test complex)	November 2, 1999 (ABM test launch, 53T6) October 2, 2002 (ABM test launch, 51T6) November 29, 2004 (ABM test launch, 53T6) December 5, 2006 (ABM test launch, 53T6) October 11, 2007 (ABM test launch, 53T6) October 30, 2007 (ABM test launch, 53T6) October 29, 2009 (ABM test launch, 53T6) December 20, 2011 (ABM test launch, 53T6M) October 30, 2013 (ABM test launch, 53T6) May 8, 2014 (ABM test launch, 53T6) June 9, 2015 (ABM test launch, 53T6) June 21, 2016 (ABM test launch, 53T6) June 16, 2017 (ABM test launch, 53T6 or 53T6M)

Figure 22 - Sary Shagan

Site 35 at possesses two silos for conducting test and training launches of the 53T6 ABM.

Baikonur

Function:	**Associated Programs:**
Space launch center and missile test complex	IS
Coordinates:	**Key Dates:**
46.079749 N 62.932500 E (Site 90, IS launch complex)	October 27, 1967 (first test launch of IS ASAT)

Figure 23 - Baikonur

Site 90 was operated as a test launch site for the IS ASAT program, using the UR-200 and Tsyklon-2A boosters.

United States

Fort Greely

Function:	**Associated Programs:**
ABM complex	GMD
Coordinates:	**Key Dates:**
63.953987 N -145.725365 W	

Figure 24 - Fort Greely

Fort Greely possesses forty silos for the GBI missile, the interceptor component for the GMD system.

Vandenberg Air Force Base

Function:	**Associated Programs:**
Space launch center and ABM complex	GMD
Coordinates: 34.751622 N -120.619366 W (SLC 2E) 34.755560 N -120.622473 W (SLC2W) 34.640221 N -120.589544 W (SLC 3E) 34.581422 N -120.626792 W (SLC 6) 34.739657 N -120.619205 W (LC 576-E)	**Key Dates:**

Figure 25 - Vandenburg

Vandenberg Air Force Base houses various launch facilities used to deliver military payloads into orbit.

Cape Canaveral

Function:	**Associated Programs:**
Space launch center	
Coordinates:	**Key Dates:**
28.583414 N 80.582891 W (SLC 41) 28.532311 N 80.566601 W (SLC 37)	

Figure 26 - Cape Canaveral

Cape Canaveral houses various launch facilities used to deliver military payloads into orbit.

Kwajalein Atoll

Function:	**Associated Programs:**
ABM test site	GMD
Coordinates:	**Key Dates:**
09.005828 N 167.726986 E (Meck Island)	

India

Satish Dhawan

Function:	**Associated Programs:**
Space launch center	
Coordinates:	**Key Dates:**
13.733280 N 80.234840 E (First Launch Pad) 13.719751 N 80.230431 E (Second Launch Pad)	

Figure 27 - Satish Dhawan

Satish Dhawan is India's primary space launch center and could have a role in future ASAT development.

Wheeler Island

Function:	**Associated Programs:**
Missile test complex	AAD, PAD, PDV
Coordinates:	**Key Dates:**
20.755135 N 87.088511 E (Launch Complex IV)	December 6, 2007 (AAD ABM test) March 6, 2009 (PAD ABM test) March 15, 2010 (AAD ABM test) July 26, 2010 (AAD ABM test) March 6, 2011 (AAD ABM test) November 23, 2012 (AAD ABM test) April 27, 2014 (PDV ABM test) April 6, 2015 (AAD ABM test) November 22, 2015 (AAD ABM test) May 15, 2016 (AAD ABM test) February 11, 2017 (PDV ABM test)

Figure 28 - Wheeler Island

The Integrated Test Range complex at Wheeler Island is the primary test site for India's antiballistic missile systems.

Sensor Complexes

China

Radar complexes

Site:
Large phased-array radar (LPAR) sites

Coordinates:
46.527890 N 130.755269 E
36.024737 N 118.091972 E
30.286623 N 119.128566 E
41.641212 N 86.236834 E

Figure 29 - LPAR site near Hangzhou

The above image shows a Chinese LPAR emplaced west of Hangzhou. China operates numerous LPARs which could serve as acquisition sensors for ABM and/or ASAT systems.

Space surveillance complexes

Site:
Zhanyi space tracking site

Coordinates:
25.637529 N 103.713979 E

Radar complexes

Site:
Voronezh radar sites

Coordinates:
60.275210 N 30.545593 E (77Ya6M)
51.273673 N 58.959036 E (77Ya6M)
58.506337 N 92.045261 E (77Ya6DM)
53.139759 N 83.680803 E (77Ya6DM)
54.857482 N 20.182510 E (77Ya6DM)
44.925428 N 40.983915 E (77Ya6DM)
52.855571 N 103.232513 E (77Ya6VP)
67.613910 N 63.752342 E (under construction)

Figure 30 - Voronezh at Mishelvka

The image above shows the two Voronezh-VP arrays at Mishelevka near Irkutsk. The Voronezh-VP replaced a Daryal radar.

Site:
Daryal/Volga radar sites

Coordinates:
40.870203 N 47.801353 E (Daryal)
65.209966 N 57.285247 E (Daryal)
52.848887 N 26.470524 E (Volga)

Site:
Dnestr/Dnepr/Daugava radar sites

Coordinates:
52.874943 N 103.260566 E (Dnestr)
52.877874 N 103.272584 E (Dnepr)
46.603278 N 74.530860 E (Dnepr)
68.113720 N 33.910522 E (Daugava)

Figure 31 - Dnestr/Dnepr Site at Mishelevka

The above image shows Dnestr and Dnepr radar arrays at Mishelevka near Irkutsk. Dnestr arrays were initially placed here to form complex SD-1 intended to serve as satellite detection systems.

Figure 32 - Daugava/Dnestr-M Site at Olenegorsk

The above image shows the Daugava receiver array installed at the Olenegorsk Dnestr-M radar site. Daugava was a trial version of the later Daryal system. The Dnestr and Daugava will be replaced by a Voronezh-series radar system in the near future.

Site:
ABM network radar sites

Coordinates:
56.173299 N 37.769327 E (Don-2N)
55.219146 N 37.294505 E (Dunai-3M)

Site:
Krona sites

Coordinates:
43.826155 N 41.343355 E
42.935368 N 132.576247 E

Figure 33 - Krona Complex near Nakhodka

The above image shows the Krona complex near Nakhodka. Krona employs various sensors to serve as a satellite identification and tracking complex.

Site:
Okno site

Coordinates:
38.280551 N 69.224786 E

Site:
30J6 complex

Coordinates:
43.718100 N 41.227653 E

United States

Space surveillance complex

Site:
Schriever Air Force Base

Coordinates:
38.801895 N -104.526120 W

India

Radar complex

Site:
Green Pine/Swordfish radar sites

Coordinates:
19.854052 N 85.969496 E
13.195549 N 78.173603 E

Iran

Space surveillance complex

Site:
Delijan

Coordinates:
34.119728 N 50.877829 E

To learn more about Secure World Foundation

please visit www.swfound.org