GLOBAL COUNTERSPACE CAPABILITIES

—

AN OPEN SOURCE ASSESSMENT

Editors

—

Brian Weeden
Director Of Program Planning

Victoria Samson
Washington Office Director

APRIL 2021

SECURE WORLD FOUNDATION

Table of Contents

LIST OF FIGURES

LIST OF TABLES

ABOUT SECURE WORLD FOUNDATION

Secure World Foundation (SWF) is a private operating foundation that promotes cooperative solutions for space sustainability and the peaceful uses of outer space.

The Foundation acts as a research body, convener, and facilitator to promote key space security and other space related topics and to examine their influence on governance and international development.

↗

About the Editors

DR. BRIAN WEEDEN

Dr. Brian Weeden is the Director of Program Planning for Secure World Foundation and has more than 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, a former member of the Advisory Committee on Commercial Remote Sensing (ACCRES) to the National Oceanic and Atmospheric Administration (NOAA), and the Executive Director of the Consortium for Execution of Rendezvous and Servicing Operations (CONFERS).

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

Ms. Victoria Samson is the Washington Office Director for Secure World Foundation and has more than 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, the BBC, 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.

LIST OF ACRONYMS

AAD
Advanced Area Defense

ABL
Airborne Laser

ABM
Anti-Ballistic Missile

ACCRES
Advisory Committee on Commercial Remote Sensing

ADRV
Advanced Debris Removal Vehicle

AEOS
Advanced Electro-Optical System

AIS
Automated Identification System

AKM
Apogee Kick Motor

ALCOR
ARPA Lincoln C-band Observables Radar

AMS
Academy of Military Sciences

ANGELS
Automated Navigation and Guidance Experiment for Local Space

APOSOS
Asia-Pacific Ground-Based Space Object Observation System

APSCO
Asia-Pacific Space Cooperation Organization

APT
Advanced Persistent Threat

ASAT
Antisatellite

ASPOS OKP
Automated Warning System on Hazardous Situations in Outer Space

ATBM
Anti-Tactical Ballistic Missile

AWACS
Airborne Early Warning and Control Systems

BMD
Ballistic Missile Defense

BMEWS
Ballistic Missile Early Warning System

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

CFSCC
Combined Force Space Component Command

CIC
Commercial Integration Cell

CMOS
Complementary Metal-oxide Semiconductor

CNE
Computer Network Exploitation

COIL
Chemical Oxygen Iodine Laser

COMSAT
Communications Satellite

CSpOC
Combined Space Operations Center

DA-ASAT
Direct-Ascent ASAT

DARPA
Defense Advanced Research Projects Agency

DART
Demonstration for Autonomous Rendezvous Technology

DDOS
Distributed Denial of Service

DEW
Directed Energy Weapons

DHS
Department of Homeland Security

DIA
Defense Intelligence Agency

DNS
Domain Name System

DRDO
Defence Research and Development Organisation

DSA
Defence Space Agency

DSC
Defensive Space Control

EAGLE
ESPA Augmented Geostationary Laboratory Experiment

ECS
Environmental Control Systems

EELV
Evolved Expendable Launch Vehicle

EKV
Exoatmospheric Kill Vehicle

ELINT
Electronic Intelligence

EMP
Electromagnetic Pulse

ESPA
EELV Secondary Payload Adapter

ESPC
Earth System Prediction Capability

EW
Electronic Warfare

FBI
Federal Bureau of Investigation

FSB
Federal Security Service

FY
Fiscal Year

GBI
Ground-based Interceptor

GEO
Geostationary Earth Orbit

GEODSS
Ground-based Electro-Optical Deep Space Surveillance

GLONASS
Global Navigation Satellite Systems

GMD
Ground-based Missile Defense

GNSS
Global Navigation Satellite Systems

GPS
Global Positioning System

GRAVES
Grand Réseau Adapté à la Veille Spatiale

GSO
Geosynchronous Orbit

GSSAP
Geosynchronous Space Situational Awareness Program

GTO
Geosynchronous Transfer Orbit

HPM
High-Power Microwave

HTK
Hit-to-kill

IADC
Inter-Agency Space Debris Coordination Committee

ICBM
Intercontinental Ballistic Missile

ICS
Industrial Control Systems

ILRS
International Laser Ranging Service

IRBM
Intermediate Range Ballistic Missile

IRGC
Islamic Revolutionary Guard Corps

ISES
International Space Environmental Service

ISON
International Scientific Optical Network

ISR
Intelligence, Surveillance, and Reconnaissance

ISRO
Indian Space Research Organisation

ITU
International Telecommunication Union

JAXA
Japan Aerospace Exploration Agency

JICSpOC
Joint Interagency Combined Space Operations Center

JNWC
Joint Navigation Warfare Center

JSpOC
Joint Space Operations Center

JTF-SD
Joint Task Force Space Defense

KCNA
Korean Central News Agency

KIAM
Keldysh Institute of Applied Mathematics

KKV
Kinetic Kill Vehicle

KW
Kilowatt

LAC
Line of Actual Control

LACE
Low-Power Atmospheric Compensation Experiment

LEO
Low-Earth Orbit

LPAR
Large Phased-Array Radar

MDA
Missile Defense Agency

MEO
Medium Earth Orbit

MIRACL
Mid-Infrared Advanced Chemical Laser

Mi-TEx
Micro-satellite Technology Experiment

MITM
Man-in-the-middle

MMW
Millimeter Wave

MOSSAIC
Maintenance of space situational awareness integrated capabilities

MOTIF
Maui Optical Tracking and Identification Facility

NASIC
National Air and Space Intelligence Center

NavIC
Navigation with Indian Constellation

NAVWAR
Navigation Warfare

NESDIS
National Environmental Satellite, Data, and Information Service

NETRA
Network for Space Object Tracking and Analysis

NOAA
National Oceanic and Atmospheric Administration

NOTAM
Notice to Airmen

NPT
Nuclear Non-Proliferation Treaty

NRL
Naval Research Laboratory

NSA
National Security Agency

NSDC
National Space Defense Center

OCS
Offensive Counterspace

OSC
Offensive Space Control

OTV
Orbital Test Vehicle

PAD
Prithvi Air Defence

PARCS
Perimeter Acquisition Radar Attack System

PAVE PAWS
Precision Acquisition Vehicle Entry[a] Phased Array Warning System

PDV
Prithvi Defence Vehicle

PGM
Precision-Guided Munitions

PLA
People's Liberation Army

PMO
Purple Mountain Observatory

PNT
Positioning, Navigation, and Timing

PRAM
Photovoltaic Radio-frequency Antenna Module

QZSS
Quasi Zenith Satellite System

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

SDF
Self-Defense Forces

SDI
Strategic Defense Initiative

SDIO
Strategic Defense Initiative Office

SDMU
Space Domain Mission Unit

SDOAC
Space Debris Observation and Data Application Center

SHF
Super-High Frequency

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

SSN
Space Surveillance Network

SSS
Space Surveillance System

SST
Space Surveillance Telescope

SWF
Secure World Foundation

TEL
Transporter-erector-launcher

THAAD
Terminal High Altitude Area Defense

TRADEX
Target Resolution and Discrimination Experiment

TsNIIKhM
Central Scientific Research Institute for Chemistry and Mechanics

TT&C
Tracking, Telemetry, and Control

TT&M
Targeting, Tracking, and Measurement

UAS
Unmanned Aerial Systems

UAV
Unmanned Aerial Vehicle

UHF
Ultra-High Frequency

USAF
United States Air Force

USSF
United States Space Force

USINDOPACOM
United States Indo-Pacific Command

USSPACECOM
United States Space Command

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 increasingly 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 destructive and non-destructive counterspace capabilities in multiple countries. However, only non-destructive capabilities are actively being used in current military operations. The following provides a more detailed summary of each country's capabilities.

01 CHINA

LEGEND: NONE R SOME Y SIGNIFICANT G UNCERTAIN "?" NO DATA "–"

	R&D	TESTING	OPERATIONAL	USE IN CONFLICT
LEO Direct Ascent	G	G	G	R
MEO/GEO Direct Ascent	Y	Y	–	R
LEO Co-Orbital	Y	?	–	R
MEO/GEO Co-Orbital	Y	–	–	R
Directed Energy	G	Y	–	R
Electronic Warfare	G	G	G	?
Space Situational Awareness	G	G	G	?

There is strong evidence indicating that China has a sustained effort to develop a broad range of counterspace capabilities. China has conducted multiple tests of technologies for rendezvous and proximity operations (RPO) 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 co-orbital intercept of a target, and there is no public 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 and sustained organizational effort. Chinese DA-ASAT capability against LEO targets is likely mature and likely operationally fielded on mobile launchers. 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 there is an intent to develop it as an operational capability in the future.

China likely has significant electronic warfare (EW) counterspace capabilities against Global Navigation Satellite System (GNSS) and satellite communications, although the exact nature is difficult to determine through open sources. Chinese military doctrine places a heavy emphasis on electronic warfare as part of the broader information warfare, and in recent years, China has taken steps to integrate space, cyber, and electronic warfare capabilities under a single military command. While there is significant evidence of Chinese scientific research and development of EW capabilities for counterspace applications and some open source evidence of Chinese EW counterspace capabilities being deployed, there is no public evidence of their active use in military operations.

China is likely developing directed energy weapons (DEW) for counterspace use, although public details are scarce. There is strong evidence of dedicated research and development and reports of testing at three different locations, but limited details on the operational status and maturity of any fielded capabilities.

China is developing a sophisticated network of ground-based optical telescopes and radars for detecting, tracking, and characterizing space objects as part of its space situational awareness (SSA) capabilities. Like the United States and Russia, several of the Chinese SSA radars also serve missile warning functions. While China lacks an extensive network of SSA tracking assets outside its borders, it does have a fleet of tracking ships and is developing relationships with countries that may host future sensors. Since 2010, China has deployed several satellites capable of conducting RPO on orbit, which likely aid in its ability to characterize and collect intelligence on foreign satellites.

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. In 2015, China re-organized its space and counterspace forces, as part of a larger military re-organization, and placed them in a new major force structure that also has control over electronic warfare and cyber. 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.

02 RUSSIA

LEGEND: NONE R SOME Y SIGNIFICANT G UNCERTAIN "?" NO DATA "–"

	R&D	TESTING	OPERATIONAL	USE IN CONFLICT
LEO Direct Ascent	G	Y	–	R
MEO/GEO Direct Ascent	Y	–	–	R
LEO Co-Orbital	G	G	–	R
MEO/GEO Co-Orbital	Y	–	–	R
Directed Energy	G	Y	?	R
Electronic Warfare	G	G	G	G
Space Situational Awareness	G	G	G	?

There is strong evidence that Russia has embarked on a set of programs since 2010 to regain many of its Cold War-era counterspace capabilities. Since 2010, Russia has been testing technologies for RPO in both LEO and GEO that could lead to or support a co-orbital ASAT capability, and some of those efforts have links to a Cold War-era LEO co-orbital ASAT program. Additional evidence suggests Russia may have started a new co-orbital ASAT program called Burevestnik, potentially supported by a surveillance and tracking program called Nivelir. The technologies developed by these programs could also be used for non-aggressive applications, including surveilling and inspecting foreign satellites, and most of the on-orbit RPO activities done to date matches these missions. However, Russia has deployed two "sub-satellites" at high-velocity, which suggests at least some of their LEO RPO activities are of a weapons nature.

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 space assets. While Russia is actively testing what appears to be a new DA-ASAT capability in their Nudol system, it is not yet operational and does not appear 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, as well as use in Russia for protecting strategic locations and VIPs. New evidence suggests Russia may be developing high-powered space-based EW platforms to augment its existing ground-based platforms.

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.

Russia has sophisticated SSA capabilities that are likely second only to the United States. Russian SSA capabilities date to the Cold War and leverage significant infrastructure originally developed for missile warning and missile defense. Although some of these capabilities atrophied after the fall of the Soviet Union, Russia has engaged in several modernization efforts since the early 2000s to reinvigorate them. While the government-owned and-operated SSA capabilities are limited to the geographic boundaries of the former Soviet Union, Russia is engaging in international civil and scientific cooperative efforts that likely give it access to data from SSA sensors around the globe. Today, Russia is able to maintain a catalog of Earth-orbiting space objects in LEO that is somewhat smaller than that of the United States but has a slightly more robust catalog of HEO and GEO objects.

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. Russia has recently re-organized its military space forces into a new organization that combines space, air defense, and missile defense capabilities. Although technical challenges remain, the Russian leadership has indicated that Russia will continue to seek parity with the United States in space.

03 THE UNITED STATES

LEGEND: NONE R SOME Y SIGNIFICANT G UNCERTAIN "?" NO DATA "–"

	R&D	TESTING	OPERATIONAL	USE IN CONFLICT
LEO Direct Ascent	G	Y	–	R
MEO/GEO Direct Ascent	–	–	–	R
LEO Co-Orbital	Y	?	–	R
MEO/GEO Co-Orbital	Y	?	–	R
Directed Energy	G	Y	?	R
Electronic Warfare	G	G	G	G
Space Situational Awareness	G	G	G	G

The United States has conducted multiple tests of technologies for RPO 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 offensive counterspace system, the Counter Communications System (CCS), which is deployed globally to provide uplink jamming capability against geostationary communications satellites. The U. S. has also initiated a new program called Meadowlands to upgrade the CCS capabilities. Through its Navigation Warfare program, the United States has the capability to jam the civil signals of global navigation satellite services (GPS, GLONASS, Beidou) within a local area of operation to prevent their effective use by adversaries and has demonstrated doing so in several military exercises. The United States likely has the ability to jam military (Global Navigation Satellite System) GNSS signals as well, although the effectiveness is difficult to assess based on publicly available information. The effectiveness of U.S. measures to counter adversarial jamming and spoofing operations against military GPS signals is not known.

Over the past several decades, the United States has conducted significant research and development on the use of ground-based high energy lasers for counterspace and other purposes. We assess that there are no technological roadblocks to the U.S. operationalizing them for counterspace applications. With its SLR sites and defense research facilities, the United States possesses low power laser systems with the capability to dazzle, and possibly blind, EO imaging satellites. However, there is no indication that these potential high or low power capabilities have been operationalized.

The United States currently possesses the most robust SSA capabilities in the world, particularly for military applications. U.S SSA capabilities date to the beginning of the Cold War and leverage significant infrastructure developed for missile warning and missile defense. The core of its SSA capabilities is a robust, geographically dispersed network of ground-based radars and telescopes and space-based telescopes. The United States is investing heavily in upgrading its SSA capabilities by deploying new radars and telescopes in the Southern Hemisphere, upgrading existing sensors, and signing SSA data sharing agreements with other countries and satellite operators. The United States still faces challenges in modernizing the software and computer systems used to conduct SSA analysis and is increasingly looking to leverage commercial capabilities.

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).

The United States is undergoing a major reorganization of its military space activities as part of a renewed focus on space as a warfighting domain. 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.” This rhetoric has been accompanied by a renewed focus on reorganizing national security space structures and increasing the resilience of space systems. This has culminated in the reestablishment of U.S. Space Command (USSPACECOM) and the creation of the U.S. Space Force (USSF), which assumed the responsibilities of U.S. Strategic Command for space warfighting and Air Force Space Command (AFSPC) for operating, training, and equipping of space forces, respectively. To date, the mission of these new organizations is a continuation of previous military space missions, although some have advocated for expanding their focus to include cislunar activities and space-to-ground weapons. 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. There are recent budget proposals to conduct research and development of space-based missile defense interceptors and DEW that could have latent counterspace capabilities. The United States also continues to hold annual space wargames and exercises that increasingly involve close allies and commercial partners.

04 FRANCE

LEGEND: NONE R SOME Y SIGNIFICANT G UNCERTAIN "?" NO DATA "–"

	R&D	TESTING	OPERATIONAL	USE IN CONFLICT
LEO Direct Ascent	–	–	–	R
MEO/GEO Direct Ascent	–	–	–	R
LEO Co-Orbital	–	–	–	R
MEO/GEO Co-Orbital	–	–	–	R
Directed Energy	Y	?	?	R
Electronic Warfare	Y	?	?	?
Space Situational Awareness	Y	Y	Y	?

While France has long had a space program, as well as military satellites, it was not until recently that France had an explicit focus on offensive and defensive counterspace capabilities. The major change occurred in July 2019 with the release of the first French Space Defense Strategy, which elevated French military space organization and reassigned control of French military satellites from the French space agency to the military. The French strategy focuses on two main areas: to improve space situational awareness around French space assets and provide an active defense against threats. While some French officials suggested machine guns and laser cannons on satellites, the actual plan calls for ground-based lasers for dazzling and space-based inspection satellites.

05 INDIA

LEGEND: NONE R SOME Y SIGNIFICANT G UNCERTAIN "?" NO DATA "–"

	R&D	TESTING	OPERATIONAL	USE IN CONFLICT
LEO Direct Ascent	Y	Y	?	R
MEO/GEO Direct Ascent	–	–	–	R
LEO Co-Orbital	–	–	–	R
MEO/GEO Co-Orbital	–	–	–	R
Directed Energy	Y	?	–	R
Electronic Warfare	?	?	?	?
Space Situational Awareness	Y	Y	?	?

India has over five decades of experience with space capabilities, but most of that has been civil in focus. It is only relatively recently that India has started organizationally making way for its military to become active users and creating explicit military space capabilities. India's military has developed indigenous missile defense and long-range ballistic missile programs that could lead to direct ascent ASAT capabilities, should the need arise. India demonstrated that ASAT capability in March 2019 when it destroyed one of its own satellites. While India continues to insist that it is against the weaponization of space, it is possible that India is moving toward an offensive counterspace posture. India is reportedly in the early stages of working on directed energy weapons.

06 IRAN

LEGEND: NONE R SOME Y SIGNIFICANT G UNCERTAIN "?" NO DATA "–"

	R&D	TESTING	OPERATIONAL	USE IN CONFLICT
LEO Direct Ascent	–	–	–	R
MEO/GEO Direct Ascent	–	–	–	R
LEO Co-Orbital	–	–	–	R
MEO/GEO Co-Orbital	–	–	–	R
Directed Energy	–	–	–	R
Electronic Warfare	G	G	Y	Y
Space Situational Awareness	Y	Y	?	?

Iran has a nascent space program that includes building and launching small satellites that have limited capability. Technologically, it is 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's military appears to have an independent ability to launch satellites, separate from the civil space program. Iran has not demonstrated any ability to build homing kinetic kill vehicles, and its ability to build nuclear devices is still fairly constrained. Iran has demonstrated an EW capability to persistently interfere with commercial satellite signals, although the capability against military signals is difficult to ascertain.

07 JAPAN

LEGEND: NONE R SOME Y SIGNIFICANT G UNCERTAIN "?" NO DATA "–"

	R&D	TESTING	OPERATIONAL	USE IN CONFLICT
LEO Direct Ascent	–	–	–	R
MEO/GEO Direct Ascent	–	–	–	R
LEO Co-Orbital	–	–	–	R
MEO/GEO Co-Orbital	–	–	–	R
Directed Energy	?	–	–	R
Electronic Warfare	?	–	–	–
Space Situational Awareness	Y	Y	Y	–

Japan has long been a well-established space actor and its space activities have historically been entirely non-military in nature. In 2008, Japan released a Basic Space Law that allowed for national security-related activities in space and since then government officials have begun to publicly speak about developing various counterspace capabilities or developing military SSA capacity. Japan is currently undergoing a major reorganization of its military space activities and development of enhanced SSA capabilities to support military and civil applications. While Japan does not have any acknowledged offensive counterspace capabilities, it is actively exploring whether to develop them. Japan does have a latent ASAT capability via its missile defense system but has never tested it in that capacity.

08 NORTH KOREA

LEGEND: NONE R SOME Y SIGNIFICANT G UNCERTAIN "?" NO DATA "–"

	R&D	TESTING	OPERATIONAL	USE IN CONFLICT
LEO Direct Ascent	–	–	–	R
MEO/GEO Direct Ascent	–	–	–	R
LEO Co-Orbital	–	–	–	R
MEO/GEO Co-Orbital	–	–	–	R
Directed Energy	–	–	–	R
Electronic Warfare	G	Y	Y	?
Space Situational Awareness	?	?	?	–

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.

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.

09 CYBER CAPABILITIES

Multiple countries 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 counterspace 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 attack capabilities of leading nation-states and other actors.

2021 Additions

The following are brief summaries of the major additions for the 2021 edition of this report, broken down by country, along with a page reference to their location in the text. Individual minor changes or the impact of changes on summaries and assessments have been integrated into the text.

01 CHINA

→ Added launch of Chinese spaceplane and potential deployment of a subsatellite (pg 1-6)

→ Added SJ-17 RPO with SJ-20 and Chinasat 6B (pg 1-8)

→ Added unverified reports of Chinese counterspace jammers deployed to the LAC near the India-China border (pg 1-20)

→ Clarified the role of pulse rate in the effectiveness of directed energy weapons (pg 1-23)

→ Added additional clarification of the role of the Strategic Support Force in Chinese military space and counterspace operations (pg 1-31)

02 RUSSIA

→ Clarified the RPO activities of Cosmos 2519 and Cosmos 2521 and the relatively high velocity at which Cosmos 2523 was released (pg 2-6)

→ Added new details about the Burevestnik program including an aircraft-carried solid fuel launch vehicle for potentially deploying co-orbital ASATs (pg 2-7)

→ Added more details about the Cosmos 2543 RPO of USA 245 and public concerns from senior U.S. military leaders (pg 2-9)

→ Added the RPO between Cosmos 2543 and Cosmos 2535 and the high velocity deployment of a projectile from Cosmos 2543, along with the U.S. and U.K. characterization of it as an ASAT test, similar to the deployment of Cosmos 2523 (pg 2-10)

→ Added RPO between Cosmos 2543, Cosmos 2535, and Cosmos 2536 (pg 2-10)

→ Added Nudol DA-ASAT tests in April and December 2020, along with U.S. public statements (pg 2-17)

→ Added comment from Commander of the Russian Aerospace Forces that the S-500 will have capability against LEO satellites (pg 2-22)

- → Added a new Russian program called Tobol that is reportedly aimed at protecting Russian satellites from uplink jamming (pg 2-26)
- → Added information about the Tirada-2 and Bylina-MM mobile counterspace EW jammers (pg 2-26)
- → Added link between the development of the 1LK222 airborne laser and the U.S. withdrawal from the ABM Treaty (pg 2-30)
- → Added report of Russia testing the A-60 airborne laser dazzler against a Japanese satellite (pg 2-30)
- → Added details on the Peresvet mobile laser dazzler system, which is deployed to protect Russian mobile ICBMs (pg 2-30)
- → Added details on the Milky Way program to upgrade Russian SSA capabilities with new ground- and space-based telescopes (pg 2-37)
- → Clarified the role of the Roscosmos state corporation in military space activities (pg 2-40)
- → Added details about the organic integration of counterspace EW units into Russian Motorised Rifle Brigades (pg 2-41)
- → Added details about the Russian military space budget in 2020 (pg 2-41)

03 THE UNITED STATES

- → Added details about the SAINT satellite inspector and co-orbital ASAT program (pg 3-2)
- → Added details on OTV-6 of the X-37B, which included a potential satellite deployment and testing of an on-orbit power beaming system (pg 3-5)
- → Clarified that the operation of the X-37B is now overseen by Space Delta 9 of the U.S. Space Force, which conducts warfighting activities in space (pg 3-6)
- → Clarified that the GSSAP satellites are now controlled by the Space Delta 9 of the U.S. Space Force (pg 3-7)
- → Added the Bold Orion and High Virgo air-launched DA-ASAT tests (pg 3-11)
- → Added the Project HiHo air-launched DA-ASAT program (pg 3-11)
- → Added the Nike Zeus ground-based DA-ASAT program (pg 3-12)
- → Added the Program 437 ground-based DA-ASAT program (pg 3-12)
- → Updated plans for future Aegis and Aegis Ashore deployments (pg 3-16)
- → Added the Meadowlands update to the Counter Communications System (pg 3-18)

- → Updated deployment of GPS M-Code signals and end user terminals (pg 3-19)
- → Updated operational status of the SST telescope in Australia (pg 3-25)
- → Added deployment of ORS-5 and TDO-2 for space-based SSA (pg 3-25)
- → Added USAF interest in expanding SSA capabilities to cislunar (pg 3-26)
- → Added counterspace and deterrence aspects of the 2020 U.S. National Space Policy (pg 3-29)
- → Added details on the stand-up and organization of the U.S. Space Force and U.S. Space Command (pg 3-32)
- → Added space doctrine details from the U.S. Space Force Space Capstone Publication (pg 3-32)
- → Updated details on Operation Olympic Defender and allied participation (pg 3-34)
- → Added policy and doctrine details from the U.S. Space Command's "Commander's Strategic Vision" (pg 3-34)
- → Added update to the Unified Command Plan to include U.S. Space Command's roles and responsibilities (pg 3-34)
- → Added details on Advanced Battle Management System (ABMS) exercise to support U.S. Space Command (pg 3-35)

04 FRANCE

- → Clarified development plan for the French Space Command (pg 4-4)

05 INDIA

- → Added details about the 2019 Indian DA-ASAT test (pg 5-3)
- → Added Indian government official remarks about potential future ASAT tests at higher altitudes (pg 5-3)
- → Added information on Indian directed energy weapons research (pg 5-5)
- → Updated information on the operational status of the Indian SSA Control Centre (pg 5-5)

06 IRAN

- → Added details on the new Iranian military space launch vehicle, the Qassed (pg 6-3)
- → Added details on the creation of the Iranian Space Command (pg 6-3)
- → Added reports of GPS spoofing near the staff college for the Iranian Army (pg 6-6)

07 JAPAN

- → Added details on the successful SM-3 Block 2A intercept test (pg 7-2)
- → Added details on SSA hosted payloads from the United States to be added to future Japanese QZSS satellites (pg 7-3)
- → Updated details on the renamed National Space Policy Secretariat (pg 7-3)
- → Added details from the June 2020 Japanese "Outline of the Basic Plan on Space Policy" (pg 7-4)

08 NORTH KOREA

- → No significant developments reported

09 CYBER

- → Added conference paper detailing weaknesses in commercial geostationary satellite broadband Internet services (pg 9-8)

10 APPENDIX

- → Added appendix listing historical ASAT testing by country

11 APPENDIX

- → Refreshed the entire imagery appendix

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 in developing the original and subsequent editions. We are deeply grateful for their expertise and commitment.

CATHERINE DILL
GILLES DOUCET
JEFFREY EDMONDS
LAURA GREGO
MARISSA MARTIN
BRANDON KELLEY
JONATHAN MCDOWELL
SEAN O'CONNOR
PAVEL PODVIG
KEVIN POLLPETER
ROBERT RONCI
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, and Analytical Graphics, Inc., for assisting with some of the imagery and graphics.

Foreword

Space security has become an increasingly salient policy issue. Over the last decade, there has been growing concern from multiple governments about 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 are 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 is 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 hope. We intend to continue to publish updated editions of this publication that address these shortcomings, and work with the broader space community to improve this assessment.

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. 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. However, over the last three 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 to attack it by various means, including destructive and non-destructive;
- → 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.

In the 2020 edition, we added space situational awareness (SSA) as a separate category for each of the countries included in the report. SSA is defined as knowledge about the space environment and human space activities and generally includes detection, tracking and characterization of space objects and space weather monitoring and prediction. While SSA is not uniquely used for counterspace, it is a critical enabler for both offensive and defensive counterspace operations. In some countries, the national security version of SSA is known as Space Domain Awareness (SDA), with an added emphasis on detecting and characterizing threats.

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 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. **This edition has been updated to include events through February 2021.**

All cataloged space objects mentioned in this report are described by three separate identifiers. The first identifier is the public name of the space object as determined by official reports or documents. The second identifier is the international designator, a unique code established by the Committee on Space Research (COSPAR) of the International Council for Science, and consisting of the year of launch, a 3-digit incrementing launch number of that year, and up to a 3-letter code representing the sequential identifier of a piece in a launch. The third identifier is the unique number assigned to the object by the U.S. military in their public satellite catalog, often referred to as the satellite number or satno, which increments by one for each new object cataloged. In this text, first mention of a space object will include all three identifiers in the format <name> (international designator, satno). Further mentions will include only the public name if it is known or the catalog number if the public name is not known.

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 cyber or DEW, 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 are two appendices: one which includes imagery of major testing sites and facilities discussed in the report, and one that lists historical ASAT tests by country.

01 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 confirmed public evidence of China actively using counterspace capabilities in current military operations.

The following sections provide details on China's development of co-orbital, direct ascent, electronic warfare, directed energy, and space situational awareness capabilities for counterspace applications and the policy, doctrine, and military organizational framework to support those capabilities.

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, 2010-027A, 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 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 3.1).[6]

Another rendezvous between two Chinese satellites in LEO occurred in 2013. On July 19, 2013, China placed three payloads into roughly similar orbits around 670 km altitude and 98 degrees inclination from the same launch: Shiyan 7 (SY-7, 2013-037A, 39208), Chuangxin 3 (CX-3, 2013-

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://englishcricn/6909/2010/

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, https://www.thespacereview.com/article/1689/1

6 “Overview of the DART Mishap Investigation Results,” NASA, accessed March 22, 2018. http://www.nasa.govpdf/148072main_DART_mishap_overview.pdf.

037B, 39209), and Shijian 15 (SJ-15, 2013-037C, 39210). The mission was publicly described by the Chinese government as "conducting scientific experiments on space maintenance technologies." 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. 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 (USAF)'s Space-Based Surveillance System (SBSS) satellite. 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. Once on orbit, the three satellites were cataloged as Payload A, Payload B, and Payload C by the U.S. military.

More than 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 on the following page. 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.

Another rendezvous between two Chinese satellites in LEO occurred in 2013. On July 19, 2013, China placed three payloads into roughly similar orbits around 670 km altitude and 98 degrees inclination from the same launch: Shiyan 7 (SY-7, 2013-037A, 39208), Chuangxin 3 (CX-3, 2013-037B, 39209), and Shijian 15 (SJ-15, 2013-037C, 39210). 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 (USAF)'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, Payload B, and Payload C by the U.S. military.[11]

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.vphp?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/docsdat/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.

01

12 Posting on Novosti Kosmonavtiki forums, January 1, 2016, https://forum.novosti-kosmonavtiki.ru/index.php?msg=1462007.

More than 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.

FIGURE 01 - CO-ORBITAL SY-71

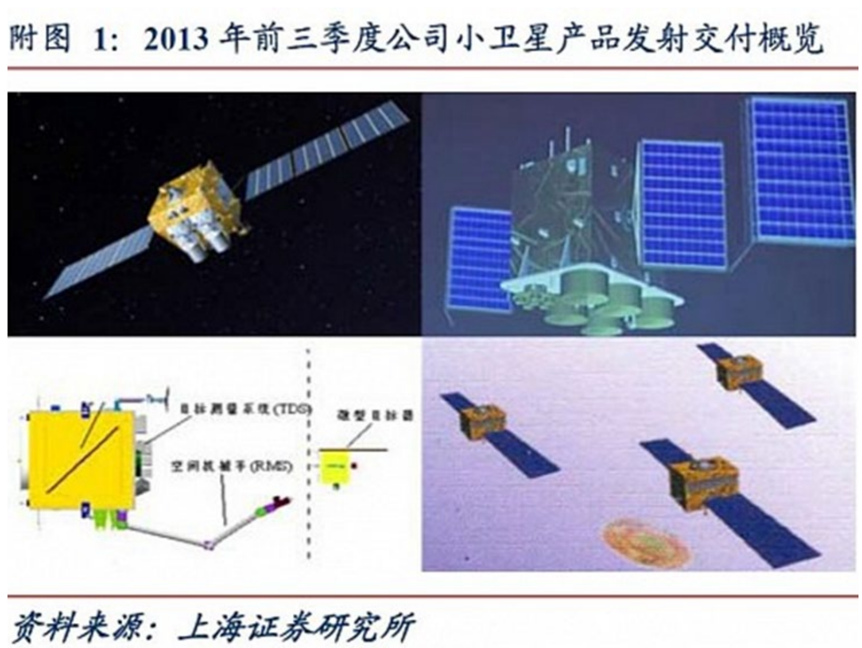


Image of the SY-7 (lower left, with robotic arm) and its small companion satellite.
Image credit: Liss[12]

In August 2013, the SJ-15 initiated a series of maneuvers to alter its orbit and bring it close to two other satellites. On August 9, the SJ-15 altered its altitude by a few tens of kilometers, which meant it passed above the CX-3 at a distance of a few kilometers before returning largely to its original orbit. On August 16, the SJ-15 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.[13] Anonymous U.S. officials claimed that the rendezvous was part of a "covert anti-satellite weapons development program," and that one of the satellites "grabbed" another,[14] although there's no way to confirm a physical docking from the publicly available tracking data and the satellite with the arm, SY-7, was not involved in this particular RPO.

On October 18, 2013, the SY-7 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). The SY-7 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.[15] 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, the SJ-15 began another series of small maneuvers to once again conduct proximity operations around the CX-3. Between April 12-14, the SJ-15 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.[16] Over the course of the rest of May, the SJ-15 slowly decreased the distance to the SJ-7 to within a kilometer.[17]

The SJ-15 continued to occasionally make changes to its orbit in 2015 and 2016, but the reasons for doing so were unclear. On December 3, 2015, the SJ-15 increased its inclination by 0.3 back to 98 degrees. On May 6, 2016, the SJ-15 changed its altitude by several tens of kilometers to once again bring it close to the CX-3.[18]

In 2016, another Chinese satellite was launched that again created concerns about on-orbit grappling. The Aolong-1 (AL-1, 2016-042F, 41629), 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

13 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/.

14 Bill Gertz, "China Testing New Space Weapons," The Washington Free Beacon, October 2, 2013, http://freebeacon.com/national-security/china-testing-new-space-weapons/.

15 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/.

16 Posting on Novosti Kosmonavtiki forums, May 5, 2014, http://novosti-kosmonavtiki.ru/forum/messages/forum12/topic13702/message1254275/#message1254275.

17 Posting on Novosti Kosmonavtiki forums, May 29, 2014, http://novosti-kosmonavtiki.ru/forum/messages/forum12/topic13702/message1262548/#message1262548.

18 Posting on NASAspaceflight.com forums, June 7, 2016, http://forum.nasaspaceflight.com/index.php?PHPSESSID=iamdpaq7ig407ooqdmi8gm06k6&topic=30486.msg1545873#msg1545873php?PHPSESSID=iamdpaq7ig407ooqdmi8gm06k6&topic=30486.msg1545873#msg1545873.

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 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 U.S. 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]

In September 2020, China launched an experimental spaceplane that may have deployed at least one small satellite on orbit. On September 4, 2020, China launched what it called a "reusable experimental spacecraft into orbit on a CZ-2F rocket from Jiuquan Satellite Launch Center under unusually heavy secrecy.[25] Few facts are known, but the U.S. military cataloged the spaceplane (PRC Test Spacecraft, 2020-063A, 46389) and a CZ-2F upper stage (CZ-2F R/B, 2020-063B, 46390) in a 348 km by 331 km and 50.2° inclination orbit.

One day later, they cataloged three pieces of debris in a similar orbit and the following day, on September 6, the U.S. military cataloged an unknown payload in orbit (Object A, 2020-063G, 46395) while also indicating the spaceplane had re-entered the atmosphere.[26] Outside experts suggested that the spaceplane could have landed on a long runway constructed at China's Lop Nor nuclear test site.[27] The mission of the small satellite it deployed is unknown.

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 concernsthat "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/.

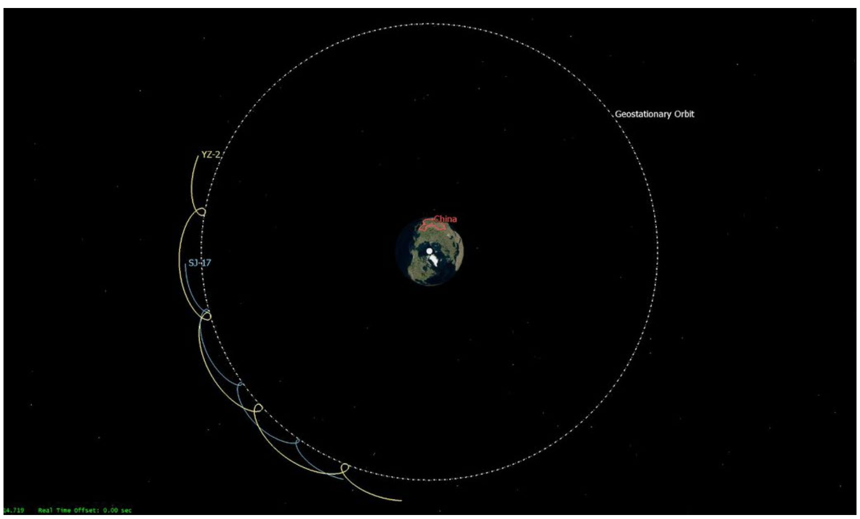
25 Geoff Brumfiel, "New Chinese Space Plane Landed At Mysterious Air Base, Evidence Suggests," NPR, September 9, 2020, https://www.nprorg/2020/09/09/911113352/new-chinese-space-plane-landed-at-mysterious-air-base-evidence-suggests.

26 Data compiled from the public U.S. military satellite catalog at https://space-track.org.

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

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 (2016-065A, 41838) 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 surveillance sensor.[28] The launch was typical of the historical process of getting most satellites to GEO using chemical propulsion,[29] taking about 6 hours and 14 minutes after launch.[30] The only anomaly was with the Yuanzheng-2 (YZ-2, 2016-065C, 41840) 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 as shown in Figure 2 below.

FIGURE 02 - ORBITAL TRAJECTORY OF THE YZ-2



Simulation of the upper stage as it periodically intrudes on the active GEO belt.
Image credit: AGI.[31]

28 "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/.

29 The other major method of getting to GEO utilizes constant thrust ion propulsion, which can take weeks or months.

30 "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/.

31 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.

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).[32] 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 commercial satellite communications services for southeast Asia.[33] 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.[34] The two satellites remained close until December 29, when Analytical Graphics, Inc, (AGI) reported that Chinasat 5A had begun drifting away.[35] 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 and moved to RPO with Chinasat 20 (2003-052A, 26643), a Chinese military communications satellite that was still under longitudinal control but had slowly been increasing in inclination for years.[36]

Over the first half of 2018, the SJ-17 made additional unusual changes to its orbit. Beginning on January 23, 2018, the SJ-17 raised its inclination from 0.43 to roughly four degrees, before reversing back to zero between July 20-22.[37] According to the commercial SSA company AGI, this reversal in inclination was also accompanied by maneuvering to a drift orbit of four degrees per day. This appears to be linked to an unexplained anomaly in the orbital trajectory of Chinasat 1C, a Chinese communications satellite launched in December 2015, which began drifting westward at 0.5 deg/day.[38] The sudden, large change in inclination suggests the SJ-17 has significant delta-vee capability as plane change maneuvers are among the most energy intensive. SJ-17 slowed to rendezvous with Chinasat 1C, coming to within 1.5 km on July 29. Ten days later, Chinasat 1C halted its drift and began to slowly drift back to its operational location. SJ-17 remained with Chinasat 1C through the first week of August before departing, while Chinasat 1C arrived back at its original location on September 7. This strongly suggests that SJ-17 was used to inspect Chinasat 1C to determine the source of the anomaly and then monitor the recovery attempt.

32 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.

33 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.

34 "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/.

35 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.

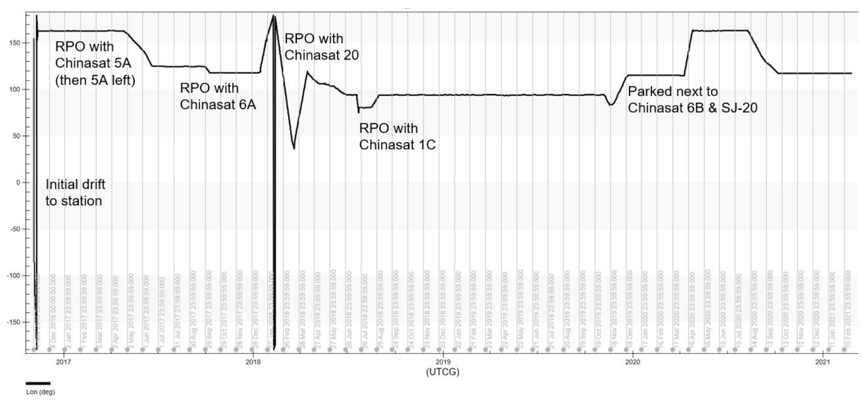
36 Posting by Liss on NASA Spaceflight.com Forum, February 6, 2021, https://forum.nasaspaceflight.com/index.php?topic=39415.msg2189039#msg2189039.

37 Jonathan McDowell, "Jonathan's Space Report," No. 754, October 8, 2018, http://planet4589.org/space/jsr/back/news.754.txt;
Verified by data compiled from the public U.S. military satellite catalog at https://space-track.org.

38 Bob Hall, "Ep16 – Chinasat 1C Space Activities," Analytical Graphics, Inc, July 2, 2019, https://www.youtube.com/watch?v=oTmRjcac3VE

Following its rendezvous with Chinasat 1C, the SJ-17 made smaller changes to RPO with Chinasat 6B in January 2020 and, SJ-20, a new Chinese high bandwidth communications satellite launched in December 2019, in October 2020. Figure 3 below summarizes the longitudinal history of the SJ-17 in the geosynchronous region.

FIGURE 03 - LONGITUDINAL HISTORY OF THE SJ-17[39]



The longitudinal history of the SJ-17 satellite since launch in 2017, including major RPOs with other satellites. Image credit: COMSPOC Corporation.

On December 23, 2018, China launched another mission to GEO that has also exhibited unusual behavior. Like its predecessors, the Tongxin Jishu Shiyan (TJS)-3 satellite was launched from Xichang Space Launch Center into an elliptical geosynchronous transfer orbit (GTO). Few details are known publicly about the TJS series, the first of which was launched in early 2017. Chinese official media has described them as communications technology test satellites but observers believe they may also be testing missile warning sensors, deployable antennas, or other technology.[40] TJS-3 appeared to be similar in nature, and the U.S. military ended up cataloging two objects from the launch in GEO: the TJS-3 satellite (2018-110A, 43874) and a second object (2018-110C, 43917) that was assumed to be an apogee kick motor (AKM), a detachable rocket engine often used to circularize a satellite in GEO, as it was slowly drifting westward. While the modern practice is to separate and dispose of AKMs above GEO for space debris mitigation, it is not uncommon for them to be in GEO. However, shortly after the separation, object 43917 did a series of maneuvers to place it into a GEO slot at 59.07E, near TJS-3.[41] Object 43917 slowly drifted toward TJS-3 and according to AGI exhibited photometry consistent with a stabilized object and not one that was tumbling.[42] Thus object 43917 appears to be a subsatellite and not an AKM, and maintaining a relatively close distance (100 to 200 km) from TJS-3.[43] In April 2019, TJS-3 departed the TJS-AKM

39 Data compiled by the COMSPOC Corporation.

40 "China opens 2017 with obscure communications satellite launch," Spaceflight101, January 5, 2017, http://spaceflight101.com/long-march-3b-tjs-2-launch/.

41 See discussion of this in the following thread on the NASASpaceflight.com forums: https://forum.nasaspaceflight.com/index.php?topic=46903.0;all.

42 Ibid.

43 Ibid.

and moved to another location, suggesting that it was conducting initial check-out for the first few months while near TJS-AKM.

The activities of the SJ-12, SJ-15, SJ-17, and TJS-3 AKM are consistent with the demonstration of RPO technologies for the purpose of satellite servicing, space situational awareness, and inspection. Notably, a counterspace assessment released by the Defense Intelligence Agency (DIA) in February 2019 stated that China is developing capabilities for inspection, repair, and space debris removal that may also be used as a weapon but did not specifically state that any Chinese RPO activities were a weapons test.[44] Specifically, they appear similar in nature to the activities of the USAF's XSS-11 satellite, which was used to do inspections of satellites in LEO in 2005 and 2006;[45] DARPA's OrbitalExpress satellite, which launched as a joined pair and conducted a series of rendezvous, docking, and robotic arm experiments in 2007;[46] the Swedish Mango (2010-028B, 36599) and Tango (2010-028F, 36827) 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;[47] and the USAF's Micro-satellite Technology Experiment (MiTEx) satellites[48] and Geosynchronous Space Situational Awareness (GSSAP) satellites,[49] which conducted inspections in the GEO belt in 2009 and 2016, respectively (See U.S. Co-Orbital ASAT; section 3.1). While the known on-orbit activities of the SJ-12, SJ-15, SJ-17, and TJS-3 AKM did not include explicit testing of offensive capabilities or

TABLE 01 - RECENT CHINESE RENDEZVOUS AND PROXIMITY OPERATIONS

DATE	SYSTEM(S)	ORBITAL PRAAMETERS	NOTES
June – Aug. 2010	SJ-06F, 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 it performed maneuvers with and may have 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.
Jan.-April 2019	TJS-3, TJS-3 AGM	35,600 km; 0°	TJS-3 AKM separated from the TJS-3 in the GEO belt and both performed small maneuvers to maintain relatively close orbital slots.

44 Defense Intelligence Agency, "Challenges to Security in Space," February 2019, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf

45 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.

46 Lt Col Fred Kennedy, "Orbital Express Space Operations Architecture," DARPA Tactical Technology Office, accessed March 23, 2018, http://archive.darpa.mil/orbitalexpress/index.html.

47 "Prisma," OHB Sweden, accessed March 23, 2018, http://www.ohb-sweden.se/space-missions/prisma/.

48 Craig Covault, "Secret inspection satellites boost space intelligence ops," Spaceflight Now, January 14, 2009, http://www.spaceflightnow.com/news/n0901/14dsp23/.

49 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/.

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.[50]

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.

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 and sustained organizational effort. Chinese DA-ASAT capability against LEO targets is likely mature and may be operationally fielded on mobile launchers. 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 (ABM) 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.[51]

These various subsidiaries have, over time, been consolidated into large state-owned companies, yet have retained deep-seated direct ties to

50 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

51 Gregory Kulacki, "Anti-Satellite (ASAT) Technology in Chinese Open-Source Publications," Union of Concerned Scientists, July 1, 2009, https://ucsusa.org/sites/default/files/2019-09/Kulacki-Chinese-ASAT-Literature-6-10-09.pdf

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.[52]

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 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.[53] 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.[54] 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 13. The first known tests were in 2005 and 2006, both from Xichang Satellite Launch Center in Sichuan (See Xichang; page 10-6), and appear to have been tests of the missile itself.[55] On January 11, 2007, the SC-19 was tested for the third time from Xichang and destroyed an aging Chinese FengYun 1C weather satellite (1999-025A, 25730) at an altitude of 865 km, which created several thousand pieces of orbital debris.[56] The system was reportedly tested again in 2010 and 2013 from the Korla Missile Test Complex (See Korla West; page 10-3) 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.

52 Ibid.

53 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.

54 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/research/assessment-chinas-anti-satellite-and-space-warfare-programs-policies-and-doctrines.
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.

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

56 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.

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.[57] 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.[58]

The organizational history of the SC-19 yields further clues. Chinese rocket development is centralized in two state-owned corporations.

FIGURE 04 - DF-21 MRBM

Missile version upon which the SC-19 is likely based, mounted atop a TEL.
Image credit: Defence Blog.[59]

[57] 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 "DF-21 (Dong Feng-21 / CSS-5)", Missile Threat, Center for Strategic and International Studies, https://missilethreat.csis.org/missile/df-21/ 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.

[58] 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/oaioai?verb=getRecord&metadataPrefix=html&identifier=ADA517485.

[59] 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.

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).[60] 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.

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, which the Chinese Academy of Sciences stated was a high-altitude scientific research mission.[61] 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,"[62] but unofficial U.S. government sources say it was actually a test of a new ballistic missile related to China's ASAT program.[63] 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 a GEO launch trajectory,[64] 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.[65] 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,[66] 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".[67] 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

60 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.

61 "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.

62 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.

63 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/.

64 "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.

65 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.

66 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.

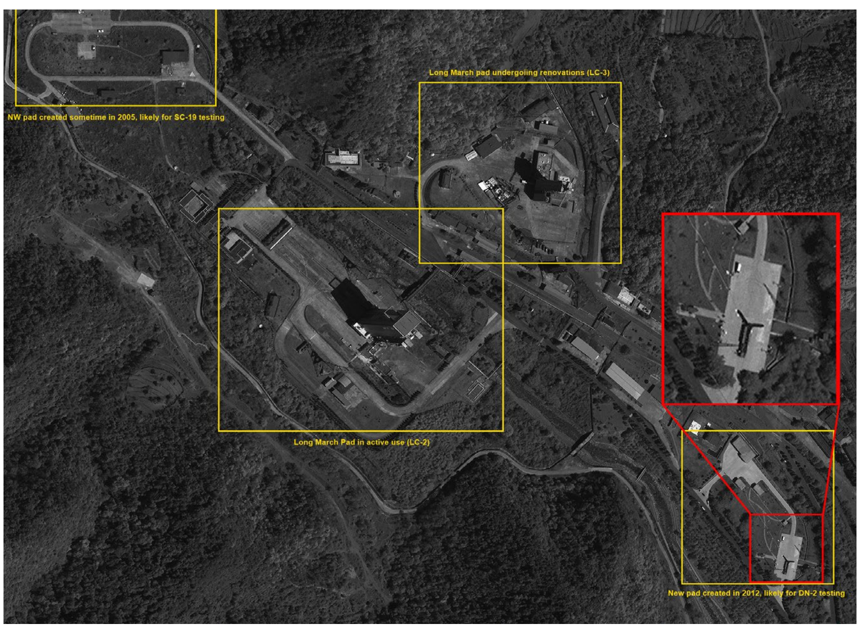
67 Andrea Shalal-Esa, "U.S. sees China launch as test of anti-satellite muscle: source," Reuters, May 15, 2013, https://www.reuters.com/article/us-china-launch/u-s-sees-china-launch-as-test-of-anti-satellite-muscle-source-idUSBRE94E07D20130515

Indian Ocean.[68] 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 5 below.[69] 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.[70] However, the only known sources of this designation are news reports that cite anonymous U.S. defense officials,[71] so the veracity of the label is in question.

In 2014, China conducted another rocket test, this time claiming that it was part of a missile defense interceptor program.[72] Very little

FIGURE 05 - XICHANG FROM APRIL 03, 2013



Imagery shows a TEL on the southeast pad.

68 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.

69 Ibid.

70 "USCC 2015 Annual Report," pp. 294-294, November 2015, https://www.uscc.gov/annual-report/2015-annual-report-congress

71 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/.

72 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/.

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. When 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 you the United States has high confidence in its assessment, that the event was indeed an ASAT test."[73] 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.[74]

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.[75] Photos from another test on July 22, this time launched from Jiuquan Satellite Launch Center (See Jiuquan, page 10-1) were captured by a pilot on a Dutch commercial airliner flying over the Himalayas.[76] On February 5, 2018, Chinese state media announced it had carried out "land-based mid-course missile interception test within its territory."[77] 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).[78] 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.[79]

More recent reporting suggests that at least one of these systems, likely the SC-19, has achieved operational status. In December 2018, the National Air and Space Intelligence Center (NASIC) released a public counterspace assessment of foreign space and counterspace capabilities that stated, "China has military units that have begun training with anti-satellite missiles."[80] In his statement for the record before the United States Senate on January 29, 2019, Director of National Intelligence Daniel Coats stated that China "has an operational ground-based ASAT missile intended to target low-Earth-orbit satellites."[81] Taken together, these statements suggest that China has operationally deployed DA-ASAT systems to at least some units and has developed operational training for their use, although there has not been independent confirmation of this through open sources.

73 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/.

74 "USCC 2015 Annual Report," pg. 293, November 2015, accessed March 23, 2018, https://www.uscc.gov/annual-report/2015-annual-report-congress

75 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.

76 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/.

77 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/.

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

79 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/.

80 National Air and Space Intelligence Center, "Competing in Space", December 2018, https://media.defense.gov/2019/Jan/16/2002080386/-1/-1/1/190115-F-NV711-0002.PDF.

81 Daniel Coats, "Worldwide threat assessment of the United States intelligence community," Senate Select Committee on National Intelligence, January 29, 2019, https://www.intelligence.senate.gov/sites/default/files/documents/os-dcoats-012919.pdf.

TABLE 02 - HISTORY OF CHINESE DA-ASAT TESTS[82]

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. 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	Unknown 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

82 Data compiled from multiple sources already cited in the text of this document.

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 3.2) or Russian Kontakt (See Russian Direct-Ascent ASAT; section 2.2) 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.

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 of warning time before impact.

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 ELECTRONIC WARFARE

ASSESSMENT

China is likely to have significant electronic warfare (EW) counterspace capabilities against Global Navigation Satellite System (GNSS) and satellite communications, although the exact nature is difficult to determine through open sources. Chinese military doctrine places a heavy emphasis on electronic warfare as part of the broader information warfare, and in recent years, China has taken steps to integrate space, cyber, and electronic warfare capabilities under a single military command. While there is significant evidence of Chinese scientific research and development of EW capabilities for counterspace applications and some open source evidence of Chinese EW counterspace capabilities being deployed, there is no public evidence of their active use in military operations.

SPECIFICS

The following paragraphs provide a general overview of different types of EW capabilities as related to counterspace applications that are applicable to all the country-specific EW sections in this report. 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.”[83] In the context of this report, the scope of EW is narrowed to refer specifically to intentional interference with an adversary’s radiofrequency (RF) transmissions to or from a satellite. This intentional interference is often referred to as “jamming”.[84]

In the case of satellite signals, jamming is often characterized as being either uplink or downlink, as shown in Figure 5 below. 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

[83] United States Department of Defense, “DOD Dictionary of Military and Associated Terms,” Defense Technical Information Center, February 2018, pg. 78, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

[84] Ibid, pg. 76.

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.

FIGURE 06 - UPLINK VS DOWNLINK JAMMING

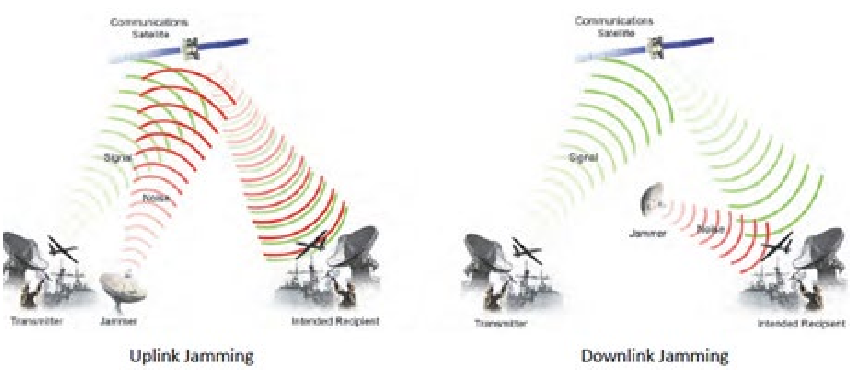


Image credit: Infosec Institute.[85]

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.

The three principal areas of concern for counterspace are the jamming of:

01. GNSS signals
02. Satellite communications
03. Synthetic aperture radar (SAR) imaging

The following sections indicate China-specific developments of these capabilities.

85 Pierluigi Paganini,"Hacking Satellites: Look Up To the Sky," Infosec Institute, September 18, 2013, https://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/#gref.

GNSS JAMMING

GNSS jamming, particularly of the U.S. GPS, is a well-known technology and jammers are widely proliferated throughout the globe. China is assessed to be proficient in GNSS jamming capabilities, having developed both fixed and mobile systems. The known systems are downlink jammers, which affect GNSS receivers within a local area. There is no publicly-known system that targets uplink jamming of GNSS satellites themselves.

In April 2018, news reports revealed satellite imagery indicating China had placed military jamming equipment on the Mischief Reef, part of the disputed Spratly Islands in the South China Sea.[86] The imagery shows what appears to be mobile military jamming trucks that are designed to interfere with GPS or other GNSS signals.

In November 2019, a new report detailed multiple incidents of GNSS jamming and spoofing near the Chinese port of Shanghai.[87] Analysts from the Center for Advanced Defense Studies determined that jamming and spoofing of the GNSS signals used by the automatic identification system (AIS) to track commercial shipping began in the summer of 2018. The attacks culminated in July 2019 with spoofed locations for over three hundred ships in Shanghai or the Huangpu River on a single day. The effect of the spoofing was also unique: the position of the ships was jumping every few minutes in a ring pattern that showed as large circles over weeks. Additional analysis showed that the spoofing was affecting fitness tracks as well, suggesting it was impacting all GPS receivers in the area.

SATCOM JAMMING

The January 2019 DIA space and counterspace report states that China is developing jammers to target SATCOM over a range of frequency bands, including military protected extremely high frequency communications, citing Chinese scientific papers describing the status of research and potential operational techniques.[88]

SAR JAMMING

The January 2019 U.S. DIA space and counterspace report states that China is developing jammers dedicated to targeting SAR aboard military reconnaissance platforms, including LEO satellites, citing Chinese scientific papers describing the status of research and potential operational techniques.[89]

In October 2020, an Indian newspaper reported that China had deployed “counterspace jammers” near Lakdah, Kashmir close to the disputed Line of Actual Control on the border between China and India.[90] The report suggests that the purpose of these jammers is to prevent satellites from tracking the deployment of Indian troops, but this has not been verified.

86 Michael Gordon and Jeremy Page, “China installed military jamming equipment on Spratly Islands, U.S. says,” The Wall Street Journal, April 9, 2018, https://www.wsj.com/articles/china-installed-military-jamming-equipment-on-spratly-islands-u-s-says-1523266320.

87 Mark Harris, “Ghost Ships, Crop Circles, and Soft Gold: A GPS Mystery in Shanghai,” MIT Technology Review, November 15, 2019, https://www.technologyreview.com/s/614689/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/

88 Defense Intelligence Agency, “Challenges to Security in Space,” January 2019, p. 20, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf

89 Ibid.

90 Shishir Gupta, “China builds new structures near LAC, relocates troops. India reads a message,” Hindustan Times, October 20, 2020, https://www.hindustantimes.com/india-news/india-spots-movement-across-lac-china-is-building-new-structures-relocating-troops/story-DIe6zUzawUyTwEBrakZ45K.html.

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, China 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 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 attractive option for China in a future conflict with the United States as it is likely to take place in the Asia-Pacific region and thus the United States would be heavily reliant on satellite communications, space-based ISR, and GNSS for successful military operations.

However, conducting operationally-useful, dependable, and reliable jamming of highly-used military space capabilities, such as GNSS, is more difficult than most commentators suggest. Military GNSS signals are much more resilient to jamming than civil GNSS signals, and a wide variety of tactics, techniques, and procedures exist to mitigate attacks.[91] It is much more likely that an EW counterspace weapon would degrade military space capabilities rather than completely deny them.

1.4 – CHINESE DIRECTED ENERGY WEAPONS

ASSESSMENT

China is likely to be developing directed energy weapons (DEW) for counterspace use, although public details are scarce. There is strong evidence of dedicated research and development and reports of testing at four different locations, but limited details on the operational status and maturity of any fielded capabilities.

SPECIFICS

Directed Energy Weapons (DEW) refers to a class of potential weapons technologies that harness concentrated beams of electromagnetic waves or subatomic particles. The three main types of DEWs are lasers, particle beams and radio frequency energy. Of these, laser systems are the most developed and most prominent of the DEW counterspace threats.

91 Brandon Davenport and Rich Ganske, "Recalculating Route: A Realistic Risk Assessment for GPS," War on the Rocks, March 11, 2019, https://warontherocks.com/2019/03/recalculating-route-a-realistic-risk-assessment-for-gps/.

[92] David Wright, Laura Grego, and Lisbeth Gronlund, The Physics of Space Security, American Academy of Arts and Science, 2005, Appendix A to Section 11, https://www.ucsusa.org/sites/default/files/2019-09/physics-space-security.pdf

LASER SYSTEMS

Laser systems for counterspace applications could be either ground-based or space-based. Ground-based systems require much higher power and have few restrictions on size, type and consumptions of chemicals or electrical power. Space-based systems, on the other hand may be effective at lower power but are severely restricted in size and power availability. For example, ground-based chemical lasers can generate high power but would be difficult to implement in space due to their size and the disturbance torques that may be generated by exhaust. Solid state and fiber lasers would be more appropriate for space basing but require large inputs of electrical energy.

Although admittedly a great oversimplification, a number of essential technological building blocks are required to be developed in order to field a high-power laser that will have an effective counterspace capability:

01. High fidelity space situational awareness,
02. High power laser device,
03. Precise beam tracking and control, and
04. Adaptive optics to counteract atmospheric turbulence (ground-based)

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

01. Dazzling of a satellite's imaging sensor
02. Damage to a satellite's imaging sensor
03. Damage to 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.[92]

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 Watt laser could be sufficient to create a dazzling effect and obscure an area on the ground.[93] Other research confirms this finding, but also notes that the pulse rate of the laser needs to be taken into account, as the laser could only impact a satellites' optics if they were pointed at the laser during a pulse.[94] 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 as 40 Watts. 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 kilowatt range.[95]

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.

93 Ibid.

94 Yousaf Butt, "Effects of Chinese Laser Ranging on Imaging Satellites," Science and Global Security, 17:20-35, 2009, http://scienceandglobalsecurity.org/archive/sgs17butt.pdf

95 Ibid.

NEUTRAL PARTICLE BEAMS

High energy particle beams are generated by accelerating and focusing subatomic particles through the use of powerful electromagnetic fields. Neutral particle beams are a type of particle beam that consists of neutral particles. Neutral beams are required for counterspace applications since, unlike charged beams, they are unaffected by the Earth's magnetic field.

RADIO FREQUENCY WEAPONS

Radio frequency weapons, not to be confused with RF jammers, emit a very intense focused beam of microwave energy. The high-power microwave (HPM) energy can cause damage to electronic circuitry as well as discomfort to humans.

CHINESE DEW DEVELOPMENT AND TESTING

China has been actively pursuing DEW for counterspace and other applications since the 1960s, and there are significant scientific and technical discussions of research and possible future military applications as part of the Project 640 Anti-Ballistic Missile program.[96] However, exactly how advanced Chinese DEW counterspace weapons are is unknown and there is very little public evidence of their deployment or use.

Open source research suggests there are at least five sites supporting China's DEW work.[97] Two of these sites are the Center for Atmospheric Optics at the Anhui Institute for Optics and Fine Mechanics in Hefei, Anhui Province, and the Chinese Academy of Engineering Physics campus in Mianyang, Sichuan Province. Both facilities have strikingly similar large, rectangular buildings with retractable roofs and suggest facilities where DEW aimed at satellites could have been developed. The third site is located near the Korla Missile Test facility in Xinjiang Province and features camouflaged buildings and security fences that strongly suggest it is military-operated. In March 2019, a retired Indian Air Force officer published an article showing commercial satellite imagery of the Xinjiang facility and four buildings suspected of housing laser weapons.[98]

In 2006, a report by Defense News cited anonymous U.S. defense officials who claimed that China had used ground-based lasers to "dazzle" or blind U.S. optical surveillance satellites on multiple occasions.[99] Subsequent reporting suggested that the satellites may have been merely illuminated by the lasers and senior U.S. officials at the time stated that no U.S. satellites were materially damaged.

In December 2013, an article in a Chinese scientific journal stated that a successful laser blinding test had been carried out in 2005 against a LEO satellite at 600 km altitude.[100]

The December 2018 NASIC counterspace assessment stated that Chinese defense research has proposed the development of several reversible and non-reversible counterspace directed-energy weapons,

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

97 Based on personal communication with Sean O'Conner.

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

99 Glenn Kessler, "Bachman's claim that China 'blinded' U.S. satellites," Washington Post, October 4, 2011, https://www.washingtonpost.com/blogs/fact-checker/post/bachmanns-claim-that-china-blinded-us-satellites/2011/10/03/gIQAHvm7IL_blog.html?utm_term=.1bdb2e34aa46.

100 Gao Min-hui, Zhou Yu-quan and Wang Zhi-hong, "Development of Space Based Laser Weapons," Chinese Optics, December 2013, http://chineseoptics.net.cn/en/article/doi/10.3788/CO.20130606.810

101 National Air and Space Intelligence Center, "Competing in Space", December 2018, https://media.defense.gov/2019/Jan/16/2002080386/-1/-1/1/190115-F-NV711-0002.PDF.

although did not provide more specifics.[101] The January 2019 DIA space and counterspace report stated that China is likely pursuing laser weapons for counterspace applications and assessed that China will likely field a ground-based laser weapon by 2020, although this has not yet been confirmed.[102] The DIA report cites several Chinese scientific papers on DEW research or proposals for military uses but does not provide additional evidence of real-world systems.

MILITARY UTILITY

DEWs, primarily lasers, offer significant potential for military counterspace applications. They offer the possibility of interfering with or disabling a satellite without generating significant debris. The technologies required for ground-based lasers systems are well developed. Ground-based systems can dazzle or blind EO satellites, or even inflict thermal damage on most LEO satellites.

In contrast, the technical and financial challenges to space-based DEW for counterspace remain substantial. These include mass of the weapon, consumables and disturbance torques (chemical lasers), electrical power generation (solid state and fiber lasers, particle beams), target acquisition and tracking, and the potential required large size of constellation. The acquisition and tracking challenges are greatly simplified in a co-orbital GEO or LEO scenario.

However, both ground- and space-based DEW counterspace capabilities do have significant drawbacks in assessing their effectiveness. 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 a non-destructive DEW attack actually worked.

1.5 – CHINESE SPACE SITUATIONAL AWARENESS CAPABILITIES

ASSESSMENT

China is developing a sophisticated network of ground-based optical telescopes and radars for detecting, tracking, and characterizing space objects. Like the United States and Russia, several of the Chinese SSA radars also serve missile warning functions. While China lacks an extensive network of SSA tracking assets outside its borders, it does have a fleet of tracking ships and is developing relationships with countries that may host future sensors. Since 2010, China has deployed several satellites capable of conducting RPO on orbit, which likely aid in its ability to characterize and collect intelligence on foreign satellites.

SPECIFICS

SSA is the ability to accurately characterize the space environment and activities in space. Civil SSA combines positional information on the trajectory of objects in orbit (mainly using optical telescopes and

[102] Defense Intelligence Agency, "Challenges to Security in Space," January 2019, p. 20, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf

radars) with information on space weather. Military and national security SSA applications also include characterizing objects in space, their capabilities and limitations, and potential threats.

Ground-based radars have historically been the backbone of SSA. Radar consists of at least one transmitter and receiver. The transmitter emits radio waves at a specific frequency, some of which reflect off the target and are measured by the receiver, which can then calculate the location of the target in relation to the radar. The primary advantages of radars are that they can actively measure the distance to a target and some types of radars can accurately track many objects at once. Some radars can also detect the motion of an object and construct a representation of its shape. The main disadvantages of radars are their cost, size, and complexity.

Optical telescopes are also widely used for SSA. Telescopes collect light or other electromagnetic (EM) radiation emitted or reflected by an object and focused into an image using lenses, mirrors, or a combination of the two. The main advantages of using optical telescopes for SSA is their ability to cover large areas quickly and, in particular, to track objects above 5,000 km (3,100 mi) altitude. Some telescopes can create high resolution images of space objects. The main disadvantage of optical telescopes is that they require specific lighting conditions and clear skies to see an object, although space-based optical telescopes eliminate some of these limitations.

Other types of sensors can be used for SSA, including sensors that detect radio frequency (RF) or other types of signals from satellites, lasers that measure the distance or range to a satellite very accurately, and infrared sensors that detect heat. Combining data from many different types of sensors, both ground- and space-based, that are also distributed around the globe provides a more complete picture of the space environment and of activities in space.

China's main optical SSA capabilities are operated by the Purple Mountain Observatory (PMO), which operates multiple telescopes in seven separate locations that can track satellites throughout all orbital regimes.[103] PMO originated from civilian and scientific research on astronomy and maintains a strong scientific focus. Since the early 2000s, PMO has increasingly been involved in tracking human-generated space objects and orbital debris and is China's main contributor to the Inter-Agency Space Debris Coordination Committee (IADC) that does research on orbital debris.[104]

Few details are known about China's radar SSA capabilities as they are primarily operated by the PLA. The PLA operates at least five large phased-array radars (LPARs) that likely have a primary mission of ballistic missile warning but could also support a SSA mission. The existing radars are located near Huanan (46.53N, 130.76E), Yiyuan (36.02N, 118.09E), Hangzhou (30.29N, 119.13E), Korla (41.64N, 86.24E), and Kongtong (35.4829 N 106.571 E).[105] The radars are approximately 30 meters in diameter and likely have a coverage arc of 90 to 120 degrees,

[103] "About Purple Mountain Observatory (PMO)," Purple Mountain Observatory, http://english.pmo.cas.cn/au/.

[104] Charles Choi, "China Says Work Under Way to Mitigate Space Junk," Space.com, September 3, 2007, https://www.space.com/4301-china-work-mitigate-space-junk.html.

[105] Andrew Tate, "China integrates long-range surveillance capabilities," IHS Jane's, 2017, https://www.janes.com/images/assets/477/75477/China_integrates_long-range_surveillance_capabilities.pdf.

similar to a U.S. BMEWS radar (See U.S. Space Situational Capabilities; Section 3.5).[106] The Korla radar can be rotated and is likely used to support the ballistic missile and ASAT testing done at Korla.

In June 2015, China launched the Space Debris Monitoring and Application Center to collate SSA data from various sensors and help protect Chinese satellites from on-orbit collisions. The Space Debris Monitoring and Application Center, part of the China National Space Administration, is responsible for tracking waste, analyzing hazards, developing prevention and disposal plans, setting up a database and communicating with other nations and international organizations.[107] Officials stated that the Center would provide early warnings of close approaches and possible collisions to Chinese satellite operators.

China also maintains a global network of satellite tracking stations, which may have some SSA capabilities. China maintains a fleet of Yuanwang ships that are primarily used to support Chinese space launches.[108] The ships will deploy to areas around the world where they can augment China's ground-based satellite tracking, telemetry, and control (TT&C) located in its territory. In addition, China has signed agreements to host ground-based tracking stations in Karachi, Pakistan; Swakopmund, Namibia, Malindi, Kenya; Dongara, Australia; Santiago, Chile; Alcantara, Brazil; Neuquén, Argentina; and Kiruna, Sweden.[109] All of these TT&C capabilities are coordinated through the Xi'an Satellite Measurement and Control Center. Typically, TT&C facilities use antennas to detect signals from active satellites and broadcast commands to them or receive transmissions from them, which would not be able to track orbital debris or satellites broadcasting on different frequencies. These facilities may include telescopes or other SSA sensors that could do such tracking, and their spread has prompted concerns about the PLA using them for military operations or espionage.[110] However, to date there is no evidence that the international TT&C sites operated by China are fundamentally different from those operated by other countries.

In addition to its national effort, China has also engaged in international cooperation efforts on SSA through the Asia-Pacific Space Cooperation Organization (APSCO).APSCO is a China-led intergovernmental organizational for space cooperation that includes Bangladesh, Iran, Mongolia, Pakistan, Peru, Thailand, and Turkey as members and Mexico as an observer.[111] In 2012, APSCO started the Asia-Pacific Ground-Based Space Object Observation System (APOSOS) Phase 1 project to integrate data from three telescopes in Pakistan, Peru, and Iran with a Date Centre in Beijing.[112] In April 2019, APSCO kicked off the Asia-Pacific Space Science Observatories (APSSO) Project that expanded the scope of APOSOS and included plans for a future Space Debris Observation and Data Application Center (SDOAC).[113] While some publications have described APOSOS as being fully capable of providing global GEO coverage,[114] the publications from ASPCO suggest the project is still nascent and has only limited capabilities.

106 Ibid.

107 Na Chen, "Agency Set to Track, Deal with Space Junk," Chinese Academy of Sciences, June 10, 2015, http://english.cas.cn/newsroom/archive/news_archive/nu2015/201506/t20150610_148380.shtml

108 Chen Guoling and Zou Weirong, "China Advances Maritime Space Monitoring and Control Capability," Ministry of Defense of the People's Republic of China, June 23, 2017, http://eng.mod.gov.cn/news/2017-06/23/content_4783536.htm

109 Elsa Kania, "China's Strategic Situational Awareness Capabilities," Center for Strategic and International Studies, Spring 2019, https://ontheradar.csis.org/issue-briefs/china-situational-awareness/

110 Victor Robert Lee, "China Builds Space-Monitoring Base in Argentina," The Diplomat, May 24, 2016, https://thediplomat.com/2016/05/china-builds-space-monitoring-base-in-the-americas/

111 "About APSCO," Asia-Pacific Space Cooperation Organization, http://www.apsco.int/html/comp1/content/WhatisAPSCO/2018-06-06/33-144-1.shtml, accessed February 18, 2020

112 "Ground-Based Space Object Observation Network," Asia-Pacific Space Cooperation Organization, accessed February 18, 2020, http://www.apsco.int/html/comp1/content/APOSOS/2019-03-01/59-261-1.shtml

113 NewsAPSCO," Asia-Pacific Space Cooperation Organization, April 2019, http://www.apsco.int/upload/file/20190508/20190508095839232\13.pdf

114 Defense Intelligence Agency, "Challenges to Security in Space," January 2019, p. 20, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf

China's work on space weather is conducted through the National Space Weather Monitoring and Warning Centre, which was established by the Central Planning Committee in 2002 and is part of the China Meteorological Administration.[115] The Center provides daily space weather forecasts and warnings of severe space weather based mainly off sensors and payloads carried by the Feng Yung series of meteorological satellites in LEO and GEO. China is a member of the Asia-Oceania Space Weather Alliance and the International Space Environmental Service (ISES) where it shares space weather data with fourteen other countries.[116]

MILITARY UTILITY

China's existing SSA capabilities likely allow it to maintain accurate orbital positions on and characterize most LEO, MEO, and GEO space objects. This tracking information may be good enough for targeting of anti-satellite weapons, as shown by the 2007 ASAT test, although that was against a Chinese satellite that may have been providing additional information from telemetry. China's current SSA capabilities lack robust geographic coverage outside of its borders that negatively impact the quality of its trajectory propagations in LEO and ability to track satellites in GEO over Western Europe and the Americas. China's efforts to develop a global network of TT&C stations and SSA collaboration within APSCO may offset these limitations in the near future, although the utility and reliability of these efforts for military operations is unknown.

1.6 – CHINESE COUNTERSPACE POLICY, DOCTRINE, AND ORGANIZATION

ASSESSMENT

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. In 2015, China re-organized its space and counterspace forces, as part of a larger military re-organization, and placed them in a new major force structure that also has control over electronic warfare and cyber. 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.

SPECIFICS

Chinese Views on Space Warfare – Official Chinese public statements on space warfare and space weapons have remained consistent: "China

[115] "Space Weather Products," National Center for Space Weather, accessed February 18, 2020, http://www.nsmc.org.cn/NSMC_EN/Channels/100010.html

[116] "Members," International Space Environment Service, accessed February 18, 2020, http://www.spaceweather.org/ISES/rwc/rwc.html

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."[117] 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."[118] 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.[119]

Chinese Counterspace Doctrine – The Chinese military does not appear to have an official doctrine governing the use of 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.[120] More recently, U.S. intelligence officials state that the People's Liberation Army (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.[121]

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.[122] 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."[123] 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.[124]

Chinese analysts assess that the U.S. military relies upon space for 70-90 percent of its intelligence[125] and 80 percent of its communications.[126] Based on this assessment, Chinese analysts surmise that the loss of

117 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.

118 China's Military Strategy, White Paper issued by the State Council Information Office of the People's Republic of China, May 2015, http://eng.mod.gov.cn/Database/WhitePapers/.

119 "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.

120 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).

121 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.

122 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.

123 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.

124 AMS, Science of Military Strategy, p.102.

125 Jiang and Wang, Study of Space Operations, p. 150.

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

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 becoming involved in a conflict.[127]

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 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.[128] 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."[129] 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.[130]

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,"[131] but recommend that China should "strive to attack first at the campaign and tactical levels in order to maintain the space battlefield initiative."[132] 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."[133]

127 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.

128 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.

129 Ibid, p. 1.

130 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.

131 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.

132 Ibid, p.52.

133 Ibid, pp. 142-143.

Chinese Space and Counterspace Organization — In recent years, China has undertaken significant reorganization of its military space and counterspace forces. In 2016, Chinese President Xi Jinping initiated a sweeping reorganization of the PLA. Part of this reorganization included the creation of the Strategic Support Force (SSF) as the fifth military service by merging existing space, cyber and electronic warfare units under a new unified command that reports directly to the Central Military Commission. The intent is to shift the PLA's most strategic, informatized missions from a discipline-centric to domain-centric force structure and enable full-spectrum war-fighting.[134] The SSF provides oversight of the Space Systems Department, which is responsible for nearly all PLA space operations, including: space launch and support; space surveillance; space information support; and space telemetry, tracking, and control and space warfare.[135] At this point, it is unclear if the SSF also has authority for kinetic ASAT attacks or whether that remains with the PLA Rocket Force.[136]

Chinese Counterspace Budget and Exercises — 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 below $8.227 billion.[137] However, any estimate of China's spending and budget should be seen with a great deal of skepticism.

According to the U.S. Department of Defense, in 2018, China's SSF conducted the LUOYANG series of force-on-force exercises to train in a complex electronic warfare environment, although it is uncertain to what extent the exercise involved space capabilities.[138] There is no public evidence that the LUOYANG exercise was repeated in 2019.

134 John Costello, "The Strategic Support Force: Update and Overview," The Jamestown Foundation, China Brief Volume 16 Issue 19, December 21, 2018, https://jamestown.org/program/strategic-support-force-update-overview/.

135 "Military and Security Developments Involving the People's Republic of China 2020," U.S. Department of Defense, pp. 63, https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF

136 Ibid.

137 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.

138 Office of the Secretary of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019," United States Department of Defense, May 2, 2019, p. 23, https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019%20CHINA%20MILITARY%20POWER%20REPORT%20(1).PDF

02 Russia

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 as technologically advanced as their U.S. 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 U.S. 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 President Putin, Russia also has renewed political will to obtain counterspace capabilities for much the same reason 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 non-kinetic 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, electronic warfare, and space situational awareness categories, along with a summary of Russia's policy, doctrine and military organizational framework on counterspace.

2.1 – RUSSIAN CO-ORBITAL ASAT

ASSESSMENT

There is strong evidence that Russia has embarked on a set of programs since 2010 to regain many of its Cold War-era counterspace capabilities. Since 2010, Russia has been testing technologies for RPO in both LEO and GEO that could lead to or support a co-orbital ASAT capability, and some of those efforts have links to a Cold War-era LEO co-orbital ASAT program. Additional evidence suggests Russia may have started a new co-orbital ASAT program called Burevestnik, potentially supported by a surveillance and tracking program called Nivelir. The technologies developed by these programs could also be used for non-aggressive applications, including surveilling and inspecting foreign satellites, and most of the on-orbit RPO activities done to date matches these missions. However, Russia has deployed two "sub-satellites" at high-velocity, which suggests at least some of their LEO RPO activities are of a weapons nature.

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.[139] 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 (see Baikonur; page 10-10). 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.

Table 2-1 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.[140]

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

[140] Bart Hendrickx, "Naryad-V and the Soviet Anti-Satellite Fleet," Space Chronicle, Vol 69, 2016, available at https://www.semanticscholar.org/paper/Naryad-V-and-the-Soviet-Anti-Satellite-Fleet-Hendrickx/414e786666492c48af754bdf5f383e34cea77c6f

TABLE 03 - IS TESTS CONDUCTED BY THE SOVIET UNION[141]

DATE	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)	TJS-3 AKM separated from the TJS-3 in the GEO belt and both performed small maneuvers to maintain relatively close orbital slots
Feb. 25, 1971	Cosmos 394	Cosmos 397 (IS)	Successful intercept, debris created
Mar. 18, 1971	Cosmos 400	Cosmos 404 (IS)	-
Dec. 3, 1971	Cosmos 459	Cosmos 462 (IS)	First test launch of IS interceptor
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
Dec. 17, 1976	Cosmos 880	Cosmos 886 (IS)	Successful intercept, debris created
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)	Successful intercept, no debris created
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)	Successful intercept, debris created
Apr. 18, 1980	Cosmos 1171	Cosmos 1174 (IS)	Unsuccessful intercept, debris created
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)	Successful intercept, debris created

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.[142] 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.[143] IS-M also reduced attack time by increasing speed and maneuverability to allow rendezvous with the target in a single orbit.[144] 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.

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

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

142 Ibid.

143 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.

144 Laura Grego, "Á History of Anti-Satellite Programs," Union of Concerned Scientists, January 2012, https://www.ucsusa.org/sites/default/files/2019-09/a-history-of-ASAT-programs_lo-res.pdf

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,[145] 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.[146]

As with the later versions of the IS, the Naryad development was cut short by the fall of the Soviet Union.

Table 22 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.[147] A third orbital flight test from Baikonur was conducted in December, with Rockot booster delivering the Radio ROSTO amateur radio satellite (1994-085A, 23439) into a 1,900 by 2,145 km orbit.[148] 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.

TABLE 04 - 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 (See Plesetsk; page 10-7), which has had 18 successful launches and placed more than 40 satellites into orbit.[149] The Naryad upper stage was developed into the

145 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.

146 Bart Hendrickx, "Naryad-V and the Soviet Anti-Satellite Fleet," Space Chronicle, Vol 69, 2016, available at https://www.semanticscholar.org/paper/Naryad-V-and-the-Soviet-Anti-Satellite-Fleet-Hendrickx/414e786666492c48af754bdf5f383e34cea77c6f 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.

147 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.

148 Mark Wade, "Radio," Astronautix, Accessed March 22, 2018, http://www.astronautix.com/r/radio.html.

149 For an updated list of Rokot launches, see http://en.wikipedia.org/wiki/Rokot#Launch_table.

Briz-KM and Briz-M, which are mainstays of Russian space launches to GEO.[150] 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.[151] 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 IN LEO

More recently, a resurgence of Russian 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 placed three small satellites into LEO in what appeared to be another routine launch to replenish the Rodnik constellation.[152] 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 (Cosmos 2488, 2013-076A, 39483; Cosmos 2489, 2013-076B, 39484; Cosmos 2490, 2013-076C, 39485) had successfully separated from the upper stage (Breeze-KM R/B, 20113-076D, 39486). However, U.S. military cataloged a fourth payload from the launch (Cosmos 2491, 2013-076E, 39497), and over the following months, evidence emerged from official and open sources to confirm it.[153]

From launch through the end of 2019, Cosmos 2491 did not make any significant changes to its orbit and remained in a relatively high LEO altitude of 1500 km. On December 23, 2019, Cosmos 2491 did make a small maneuver of approximately 1.5 m/s, which was accompanied by the release of 18 pieces of orbital debris that were eventually cataloged by the U.S. military.[154] Given the relatively low energy of the event, it is likely that the propulsion system of Cosmos 2491 failed immediately after launch and the orbital change and fragmentation event was caused by the explosive release of the residual fuel.

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 (Cosmos 2496, 2014-028A, 39761; Cosmos 2497, 2014-028B, 39762; Cosmos 2498, 2014-028C, 39763). Two days later, hobbyist satellite observers indicated that a fourth payload (Cosmos 2499, 2014-028E, 39765) 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 (2014-028D, 39764) that placed it in orbit.[155] The process took several months, and

[150] Anatoly Zak, "Briz-K/KM," Russian Space Web, updated March 11, 2016, http://www.russianspaceweb.com/briz.html.

[151] 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/.

[152] 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.

[153] Jonathan McDowell, "Jonathan's Space Report No. 697," May 17, 2014, https://www.planet4589.org/pipermail/jsr/2014-May/000069.html

[154] Jonathan McDowell, tweet posted on January 12, 2020, https://twitter.com/planet4589/status/1216265783644389376?s=20. Total amount of orbital debris derived from from the public U.S. military satellite catalog at https://space-track.org

[155] Thread at the Novosti Kosmonavtiki forums, dated May 16, 2014, http://novosti-kosmonavtiki.ru/forum/forum12/topic14232/?PAGEN_1=5.

it was not until the end of November when Cosmos 2499 passed within a kilometer of the Briz-KM.[156] 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.[157] 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 and 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 (Gonets M11, 2015-020A, 40552; Gonets M12, 2015-020B, 40553; Gonets M13, 2015-020C, 40554) and a classified military payload (Cosmos 2504, 2015-020D, 40555). The Gonets serve as a civilian version of the Strela/Rodnik store-and-dump LEO communications constellation. Cosmos 2504 began a small series of maneuvers in early April to bring it close to the Briz-KM upper stage (2015-020E, 40556) 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 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. In late July 2016, the USAF cataloged five small pieces of debris attributed to the Briz-KM upper stage but did not release a cause. 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.[158] This suggests that Cosmos 2504 has a satellite inspection or observation mission and may have been looking for intelligence on the Chinese direct ascent interceptor program. Cosmos 2504 maneuvered again on December 10, 2019, to lower its perigee by 40 km, although the reason is not yet known.[159]

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.[160] Russian officials declared that the launch also included a "space platform which can carry different variants of payloads" which was designated Cosmos 2519 (2017-037A, 42798).[161] In late July and early August, Cosmos 2519 made a series of small maneuvers. Publicly available information strongly suggests that Cosmos 2519 has a remote sensing mission.[162] Shortly thereafter on August 23, Russian officials announced that a small satellite, designated Cosmos 2521 (2017-037D, 42919) had separated from the platform and was "intended for the inspection of the condition of a Russian satellite."[163] Subsequently, Russia reported that the satellite-inspector completed a series of proximity operations experiments and returned to the Cosmos 2519

156 Posting on the Novosti Kosmonavtiki forums, dated November 28, 2014, http://novosti-kosmonavtiki.ru/forum/messages/forum12/topic14778/message1315049/#message1315049.

157 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.

158 Anatoly Zak, "Russia Goes Ahead with Anti-Satellite System," Russian Space Web, updated December 15, 2017, http://www.russianspaceweb.com/Cosmos-2504.html.

159 Gwiz posting to the NASASpaceflight.com forums, December 11, 2019, https://forum.nasaspaceflight.com/index.php?topic=32816.msg2024319#msg2024319.

160 Anatoly Zak, "Soyuz-2-1v Launches a Secret Satellite," Russian Space Web, August 30, 2017, http://www.russianspaceweb.com/napryazhenie.html.

161 "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.

162 Bart Hendrickx, posting on the NASAspaceflight.com Forums, February 27, 2018, https://forum.nasaspaceflight.com/index.php?PHPSESSID=35dsgsej5k8tt51h7fo7re8e04&topic=43064.msg1793720#msg1793720.

163 "С запущенного в интересах Минобороны космического аппарата выведен в космос спутник-инспектор," Interfax.ru, August 23, 2017, http://www.interfax.ru/russia/576068.

host satellite on October 26.[164] On October 30, Russia announced that another small satellite, Cosmos 2523 (2017-037E, 42986), separated from Cosmos 2521 and would have a satellite inspection function but to date, it has not been proven to approach other satellites.[165] Jonathan McDowell calculated that Cosmos 2523 was released at a relative velocity of 27 meters per second (60 miles per hour).[166] Comments from senior U.S. military leadership suggest they consider the deployment of Cosmos 2523 to have been an ASAT test, given its relatively large deployment velocity.[167] Throughout March, April, and June 2018, Cosmos 2519 and 2521 conducted several RPOs of each other.[168] As of March 2018, Cosmos 2519 and Cosmos 2521 have not maneuvered to approach any other space objects but have made small adjustments to their orbits, likely to forestall natural orbital decay.[169] Cosmos 2521 eventually re-entered the atmosphere on September 12, 2019.[170] As of February 2021, Cosmos 2519 and Cosmos 2523 remain on orbit.

Further open source research done by analyst Bart Hendrickx suggests that the Cosmos 2491, 2499, 2504, and 2521 satellites are part of a project started in 2011 to develop space-based space situational awareness (SSA) capabilities and may play a supporting role for other counterspace weapons.[171] Publicly-available documents and patents suggest a link between those Cosmos satellites and procurement for a project designated Nivelir ("Dumpy level") and under the control of the Central Scientific Research Institute for Chemistry and Mechanics (TsNIIKhM), which was involved in the original IS co-orbital ASAT program. Nivelir appears to have two series of satellites under it, 14F150 (Cosmos 2519) and 14F153 (Cosmos 2491, 2499, 2504 and 2521).[172] Hendrickx also uncovered evidence suggesting there is an active Russian co-orbital ASAT program codenamed Burevestnik ("Petrel") or project 14K168, also managed by TsNIIKhM and also started in 2011.[173] Burevestnik appears to involve both ground-based infrastructure at Plesetsk Cosmodrome near Noginsk-9, which was the location of the ground control center for the Soviet-era IS co-orbital ASAT and is near the headquarters for the Russian military space surveillance network. TsNIIKhM also supplied the explosive warhead for the IS, which targeted LEO satellites. The Nivelir inspection satellites appear to use the same bus, thermal catalytic thrusters, and fuel tanks as the Burevestnik co-orbital ASATs and may also support the Burevestnik program either by testing RPO technology or providing tracking and targeting support. Additional research suggests Burevestnik might utilize low-temperature solid-fuel generators that produce nitrogen gas to defend spacecraft from attacks.[174] The aerosol created by such gas generators would have both a masking and damaging effect, most likely meaning that they could be used not only to conceal the satellite under attack from the interceptor, but also to disable some of the interceptor's systems (such as optical devices).[175] Other research discusses the use of electrostatically charged finely dispersed particles to remove oppositely-charged orbital debris in GEO, which could also have offensive applications.[176] Another possibility is that the interceptors might use explosive charges to generate fragments, as indicated by a contract given to the Krasnoarmeysk

164 Jonathan McDowell, "Jonathan's Space Report No. 742," November 25, 2017, https://www.planet4589.org/pipermail/jsr/2017-November/000116.html

165 Bart Hendrickx, posting on the NASA spaceflight.com forums, March 3, 2018, https://forum.nasaspaceflight.com/index.php?topic=43064.msg1795369#msg1795369.

166 Jonathan McDowell, "Nivelir (Kosmos-2519 et al): A new series of Russian military satellites," Jonathan's Space Page, accessed February 2, 2020, https://planet4589.org/space/plots//niv/index.html.

167 W.J. Hennigan, "Exclusive: Strange Russian Spacecraft Shadowing U.S. Space Satellite, General Says," Time.com, February 10, 2020, https://time.com/5779315/russian-spacecraft-spy-satellite-space-force/.

168 Jonathan McDowell, "Jonathan's Space Report No. 752," August 17, 2018, https://www.planet4589.org/pipermail/jsr/2018-August/000127.html

169 "U.S. Spots Maneuvers of Russian Military Satellite," TASS, August 31, 2019, https://tass.com/science/1075876.

170 "The United States Reported that Russia Lost a Military Satellite Inspector," TASS, September 13, 2019, https://tass.ru/kosmos/6882787.

171 Bart Hendrickx, posting on the NASASpaceflight.com forums, February 1, 2019, https://forum.nasaspaceflight.com/index.php?topic=43064.msg1906972#msg1906972.

172 Bart Hendrickx, posting on the NASASpaceflight.com forums, October 22, 2019, https://forum.nasaspaceflight.com/index.php?topic=48521.msg2007320#msg2007320

173 Bart Hendrickx, "Russia develops co-orbital anti-satellite capability," Jane's Intelligence Review, September 27, 2018, https://www.janes.com/images/assets/463/83463/Russia_develops_co-orbital_anti-satellite_capability.pdf.

174 Bart Hendricks, posting on the NASASpaceflight.com forums, October 22, 2019, https://forum.nasaspaceflight.com/index.php?topic=48521.msg2007320#msg2007320.

175 Ibid.

176 Ibid.

Scientific Research Institute of Mechanization (KNIIM) and a company called OOO Expotekhvzryv as part of Burevestnik.[177] Additional reports suggest Burevestnik includes a three-stage solid fuel rocket built by NPO Iskra.[178] It appears this rocket is intended to be launched from a modified MiG-31 fighter aircraft to serve as a quick-response system to place the Burevestnik ASATs into orbit (see “78M6 Kontakt” under Russia DA-ASAT, pages 2-16 to 2-18).

Another Rodnik replenishment mission was launched from Plesetsk on November 30, 2018, and once again there was a fourth object (Object E, 2018-097E, 43755) placed into orbit in addition to the three Rodnik communications satellites (Cosmos 2530, 2018-097A, 43751; Cosmos 2531, 2018-097B, 43752; Cosmos 2532, 2019-097C, 43753). While the separation profile of Object E matched the deployment of Cosmos 2504 and other inspector satellites, Russian media reports stated that the fourth object was actually a dummy payload that replaced a laser reflector satellite at the last minute.[179] Since reaching orbit, no signals or maneuvers have been detected by the fourth object, suggesting it is indeed a piece of debris or inert payload.

On July 10, 2019, Russia launched another set of four military payloads on a Soyuz-2-1v from Plesetsk, designated by the U.S. military as Cosmos 2535 (2019-039A, 44421), Cosmos 2536 (2019-039B, 44422), Cosmos 2537 (2019-039C, 44423), and Cosmos 2538 (2019-039D, 44424). Confusingly, the U.S. military cataloging of these objects is incorrect, and Cosmos 2536 is actually catalog number 44424. All four objects were registered with the United Nations in August 2019.[180] The satellites were placed into a 97.88° inclination and 612 by 623 km orbit and one of the four satellites was detected broadcasting on the same frequency as Cosmos 2521, indicating it may be part of the Nivelir program.[181] On August 1, 2019, Russia announced that two of the satellites, Cosmos 2535 and Cosmos 2536, would be engaged in satellite inspection and satellite servicing activities.[182] According to data compiled by Jonathan McDowell, the two satellites conducted a series of RPO experiments between August 7-19, 2019, with approach distances as close as 30 km before backing off to 180 to 400 km.[183] Shortly before the RPO, nine debris objects were released in the vicinity of the two satellites, with apogees as high as 1400 km, suggesting a significant energetic event. The other two satellites, Cosmos 2537 and Cosmos 2538, have not maneuvered and may be radar calibration targets. In early October 2019, several additional debris objects were detected, although it is uncertain which parent object they came from. This, along with differences between this launch and previous Nivelir missions, have led some to suspect that they may be part of the Burevestnik co-orbital ASAT program and could be involved in the testing of aerosols or charged particles. Cosmos 2535 and Cosmos 2536 continued their RPO activities in December 2019, which resulted in the release of six more debris objects. In total, 27 cataloged debris objects have been associated with this launch as of February 2021.[184]

177 Bart Hendrickx, “Burevestnik: a Russian air-launched anti-satellite system,” The Space Review, April 27, 2020, https://www.thespacereview.com/article/3931/1.

178 Bart Hendrickx, posting on the NASASpaceflight.com forums, April 8, 2020, https://forum.nasaspaceflight.com/index.php?topic=45734.msg2066800#msg2066800.

179 Иван Синергиев,“С космодрома Плесецк запущена ракета-носитель «Рокот» с военными спутниками.” Коммерсáнтъ, November 30, 2018, https://www.kommersant.ru/doc/3814723.

180 Russian Federation, “Information Furnished in Conformity with the Convention on Registration of Objects Launched into Outer Space,” ST/SG/SER.E/906, August 15, 2019, http://unoosa.org/oosa/en/osoindex/data/documents/ru/st/stsgser.e906.html.

181 Cees Bassa, tweet posted on July 12, 2019, https://twitter.com/cgbassastatus/1149662117819060224.

182 “Российский военный спутник-инспектор проверил другой космический аппарат России на орбите,” TASS, August 1, 2019, https://tass.ru/kosmos/6724059.

183 Jonathan McDowell, ”Space Activities in 2019,” January 12, 2020, pp. 25-28, https://planet4589.org/space/papers/space19.pdf.

184 Data compiled from the public catalog maintained by the U.S. military at https://Space-Track.org.

On November 25, 2019, Russia conducted another launch of a Soyuz-2-1v from Plesetsk with announced military payload on board. The satellite was cataloged by the U.S. military as Cosmos 2542 (2019-079A, 44797) in a 97.9° inclination 370 x 860 km orbit. The mission of the satellite as announced by Russia was to conduct space surveillance as well as Earth remote sensing.[185] Outside experts have indicated it is likely the second satellite in the Nivelir 14F150 series.[186] On December 6, Cosmos 2542 released a small subsatellite that was cataloged by the U.S. military as Cosmos 2543 (2019-079D, 44835) and publicly announced by Russia.[187] Cosmos 2543 remained within 2 km of Cosmos 2542 for three days before it conducted a series of maneuvers to raise its apogee to 590 km by December 16.[188] Subsequent analysis by amateur observers strongly suggests that the purpose of these maneuvers was to place Cosmos 2543 in an orbit where it can observe a classified U.S. intelligence satellite, USA 245 (2013-043A, 39232), which was launched in 2013 and is believed to be the latest generation of electro-optical imagery satellite operated by the National Reconnaissance Office. The orbits of Cosmos 2543 and USA 245 are synchronized such that Cosmos 2543 came within 20 km of USA 245 several times in January 2020 and since then periodically comes within 150 to 300 km of USA 245 while the latter is illuminated by the Sun and can observe both sides of USA 245 continuously for up to a week at a time.[189]

The close proximity of Cosmos 2543 to USA 245 sparked concerns from the U.S. military. General John Raymond, then Chief of Space Operations for the USSF and Commander of USSPACECOM, stated, “We view this behavior as unusual and disturbing”, and compared it to the 2017 separation of Cosmos 2523 that the U.S. military considers to be a weapons test.[190] In a response published by RIA Novosti, the Russian Foreign Ministry denied those accusations, claimed that they were part of a propaganda campaign against Moscow, and stated that Cosmos 2543 did not pose a threat to USA 245 and did not violate any norms or principles of international law.[191]

A few weeks later, it appears both countries made changes in their satellites’ orbits to increase the separation of the two objects. On March 11, 2020, hobbyist tracking showed USA 245 conducted a small maneuver to increase its distance from Cosmos 2542.[192] And in late April, Cosmos 2542 lowered its perigee to increase the separation and create a gradual separation in planes between the two satellites.[193]

In June 2020, Cosmos 2543 made a series of maneuvers to place it into RPO with Cosmos 2535, including close approaches within 60 kilometers.[194] A month later, the Russian Ministry of Defense issued a press report stating that the two satellites had conducted a close-up study of a domestic satellite with the help of specialized equipment on a small satellite.[195]

185 “Успешный пуск ракеты-носителя «Союз-2.1в»”, TASS, November 26, 2019, https://www.roscosmos.ru/27793/.

186 Bart Hendrickx, posting to the NASASpaceflight.com forums, November 25, 2019, https://forum.nasaspaceflightcom/index.php?topic=49501.msg2019200#msg2019200.

187 “Минобороны провело в космосе эксперимент по отделению малого спутника от другого аппарата” TASS, December 6, 2019, https://tass.ru/armiya-i-opk/7285111

188 Jonathan McDowell, ”Space Activities in 2019,” January 12, 2020, pp. 29, https://planet4589.org/space/papers/space19.pdf.

189 Initial observations and analysis were developed by multiple observers on the See-Sat mailing list as documented here http://www.satobs.org/seesat/Dec-2019/0108.html. Additional analysis provided by Michael Thompson in a tweet thread posted January 30, 2020, https://twitter.com/M_R_Thomp/status/1222990126650994698. Further analysis and by Jonathan McDowell in a tweet thread posted February 1, 2020, https://twitter.com/planet4589/status/1223420130576818176?s=20.

190 W.J. Hennigan, “Exclusive: Strange Russian Spacecraft Shadowing U.S. Spy Satellite, General Says,” Time, February 10, 2020, https://time.com/5779315/russian-spacecraft-spy-satellite-space-force/.

191 “В МИД ответили на обвинения США в преследовании американского спутника”, РИА Новости, February 17, 2020, https://ria.ru/20200217/1564880619.html.

192 Michael Thompson (@M_R_Thomp), “Cosmos 2542, the Russian inspection satellite of recent interest, was set to make another set of close passes to USA 245 sometime in the next week,” Twitter thread, March 11, 2020, https://twitter.com/M_R_Thomp/status/1237763403231440896?s=20.

193 Bart Hendrickx, posting on the NASASpaceflight.com forums, May 15, 2020, https://forum.nasaspaceflight.com/index.php?topic=49501.msg2082452#msg2082452.

194 Bart Hendrickx, posting on the NASASpaceflight.com forums, June 15, 2020, https://forum.nasaspaceflight.com/index.php?topic=49501.msg2096595#msg2096595.

195 “Успешно испытан новый военный спутник-инспектор – Минобороны России,” ИНТЕРФАКС-АВН, July 15, 2020, https://www.militarynews.ru/story.asp?rid=0&nid=534933&lang=RU.

On July 15, a small piece of orbital debris was spotted in the vicinity of the two satellites that appeared to have separated from Cosmos 2543 at a relative velocity of between 140 to 186 meters per second (313 to 415 miles per hour).[196] The U.S. military cataloged the released object (Object E, 2019-079E, 45915) on July 16 in a 783 x 504 km orbit, with Cosmos 2543 still in a 617 x 603 km orbit. Neither object has altered its orbit significantly since.

Jonathan McDowell noted that the release occurred while the objects passed over Plesetsk, a major Russian space launch and military facility.[197] The event was similar in nature to the release of Cosmos 2523 in October 2017, and eventually two more pieces of small debris were cataloged in proximity to the satellites.

In a press release, USSPACECOM characterized the event as a space-based satellite weapons test and stated that the Russian satellites "displayed characteristics of a space-based weapon."[198] The head of the United Kingdom's Space Directorate, Air Vice-Marshall Harvey Smith, also released a public statement on Twitter expressing concerns and calling on Russia to avoid further testing.[199] The following day, the Russian Ministry of Foreign Affairs again denied those claims, stating that this was part of a campaign to discredit Russia's activities in space and that Russia was committed to the peaceful exploration and use of outer space by all states.[200]

Cosmos 2535 and Cosmos 2543 remained in close proximity through August 2020, and by August 13, they were joined by Cosmos 2536.[201] In late September 2020, Cosmos 2535 and Cosmos 2536 were close enough that they are presumed to have docked.[202] In mid-October Cosmos 2536 separated away from Cosmos 2535 to a distance of 20 kilometers.[203]

RECENT RENDEZVOUS AND PROXIMITY OPERATIONS IN GEO

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 not precisely known, with manufacturer documents referring to it as "Olymp" or "Olymp-K."[204]

[196] Jonathan McDowell (@planet4589), "I have recalculated the ejection velocity of the Kosmos-2543 projectile. The delta-V between Kosmos-2543 and object 45915 is somewhere between 140 m/s and 186 m/s," Twitter thread, July 24, 2020, https://twitter.com/planet4589/status/1286831091857403904?s=20.

[197] Jonathan McDowell (@planet4589), "More on Kosmos-2543 and object 45915. The object was ejected during a pass in view of Plesetsk, as seen here", Twitter posting, July 25, 2020, https://twitter.com/planet4589/status/1287052396749881344.

[198] USSPACECOM Public Affairs Office, "Russia conducts space-based anti-satellite weapons test," United States Space Command, July 23, 2020, https://www.spacecom.mil/MEDIA/NEWS-ARTICLES/Article/2285098/russia-conducts-space-based-anti-satellite-weapons-test/.

[199] Ministry of Defence (@DefenceHQ), "Air Vice-Marshal @HarvSmyth, director of the UK's Space Directorate, has responded to a recent Russian satellite test in space", Twitter.com, July 23, 2020, https://twitter.com/DefenceHQ/status/1286312151469166592?s=20.

[200] "Comment by the Information and Press Department regarding statements by US and British officials about the testing of a Russian satellite," the Ministry of Foreign Affairs of the Russian Federation, July 24, 2020, https://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4253360.

[201] Bart Hendrickx, posting on the NASASpaceflight.com forums, August 13, 2020, https://forum.nasaspaceflight.com/index.php?topic=49501.msg2119753#msg2119753.

[202] Jonathan McDowell (@planet4589), "Kosmos-2535 and Kosmos-2536 have now been within 1 km of each other for a month (and are likely docked). Latest TLEs might suggest they are now separated again, but too early to really be sure - might just be noise in the data," Twitter.com, September 24, 2020, https://twitter.com/planet4589/status/1309225961070751745?s=20.

[203] Jonathan McDowell (@planet4589), "After 1.5 months in the close vicinity of Kosmos-2535 (and maybe docked to it) Kosmos-2536 separated from it on Oct 12 and has now retreated to 20 km from it," Twitter.com, October 16, 2020, https://twitter.com/planet4589/status/1317161112392126464?s=20.

[204] Anatoly Zak, "Proton Successfully Returns to Flight Delivering a Secret Olymp Satellite," Russian Space Web, October 19, 2015, http://www.russianspaceweb.com/olymp.html. ST/SG/SER.E/761.

Russian filings with the United Nations reference the satellite as "Luch,"[205] which is a series of Russian "bent pipe" data relay satellites, while the USAF called it Luch/Olymp (2014-058A, 40258).

The launch proceeded the same as many other Russian GEO launches. The initial set of burns placed the Briz-M upper stage and Luch payload into an initial highly elliptical GTO. Roughly 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 Luch, 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, Luch conducted a series of maneuvers that brought it close to other operational satellites around the GEO belt. The launch process left Luch 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. Luch stayed in this general area for nearly three months.

In late January 2015, Luch 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 Luch was in this area and hypothesized that it might be due to the presence of the Russian Luch 5V satellite (2014-023A, 39727), which was launched on April 28, 2014.

Around April 4, 2015, Luch 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 Luch in between two operational Intelsat satellites, Intelsat 7 (1998-052A, 25473)) at 18.2 degrees west and Intelsat 901 (2001-024A, 26824) at 18 degrees west, where it remained until mid-September.

On September 25, 2015, Luch 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. In September 2018, the French Defense Minister stated that Luch made a "too close approach" of a French-Italian military communications satellite in late 2017.[206] Jonathan McDowell noted that the satellite was likely Athena-Fidus (2014-006B, 39509) and the close approach likely happened around October 20, 2017, as part of a move to place Luch close to Paksat-1R (2011-042A, 37779), a Pakistani communications

[205] United Nations Secretariat, "Note verbale" dated 10 December 2015 from the Permanent Mission of the Russian Federation to the United Nations (Vienna) addressed to the Secretary-General, February 1, 2016, https://cms.unov.org/dcpms2/api/finaldocuments?Language=en&Symbol=

[206] John Leicester, Sylvie Corbert, Aaron Mehta, "'Espionage:' French defense head charges Russia of dangerous games in space," DefenseNews, September 7, 2018, https://www.defensenews.com/space/2018/09/07/espionage-french-defense-head-charges-russia-of-dangerous-games-in-space/.

satellite.[207] During its five years on orbit, Luch has parked near more than a dozen commercial communications satellites for periods ranging from a few weeks to nine months, and typically close enough to be within the typical ground terminal uplink window.[208] The orbital history of Luch is documented in Table 23 below. All of the recent Russian RPO activities in LEO and GEO are summarized in Table 23.

Russia also appears to have started a new initiative to develop more advanced sensor technologies for RPO. Project Numizmat was started in 2014 and appears to involve the development of a space-based ultra-wideband (UWB) radar payload.[209] UWB radar broadcasts relatively low power signals over a very wide swath of spectrum, often more than 500 megahertz. A specific type called UWB noise radar has inherent immunity from jamming, detection, and external interference.[210] Such a payload could have significant benefits for RPO and co-orbital ASAT weapons.

TABLE 05 - RECENT RUSSIAN RENDEZVOUS AND PROXIMITY OPERATIONS

DATE(S)	SYSTEM(S)	ORBITAL PARAMETERS	NOTES
Jun. 2014 –Mar. 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
Apr. 2015 – Apr. 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
Mar. – Apr. 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 – Feb. 2020	Luch, Multiple	35,600 km, 0°	Luch parked near several satellites over nearly five years, including the Russian Express AM-6, U.S. Intelsat 7, Intelsat 401, Intelsat 17, Intelsat 20, Intelsat 36, and French-Italian Athena-Fidus satellites
Aug. – Oct. 2017	Cosmos 2521, Cosmos 2519, Cosmos 2523	670 x 650 km; 97.9°	Cosmos 2521 separated from Cosmos 2519 and performed a series of small maneuvers to doinspections before redocking with Cosmos2519. Cosmos 2523 separated from Cosmos 2521 but did not maneuver on its own
Mar.-Apr. 2018	Cosmos 2521, Cosmos 2519		Cosmos 2521 conducted close approaches of Cosmos 2519
Dec. 2019 – Mar. 2020	Cosmos 2542, Cosmos 2543, USA 245	859 x 590 km; 97.9°	Cosmos 2542 released Cosmos 2543. Cosmos 2542 did station keeping with Cosmos 2542, then raised its orbit to come within 30 km of USA 245 and establish repeated close approaches within 150 km, likely for the purpose of surveillance. Cosmos 2542 also made close approaches to USD 245
Jun. – Oct. 2020	Cosmos 2543, Cosmos 2535		Cosmos 2543 rendezvoused with Cosmos 2535 and released a small object at high relative velocity. In Sept, Cosmos 2536 joined in the RPO with the other two and may have docked with Cosmos 2535

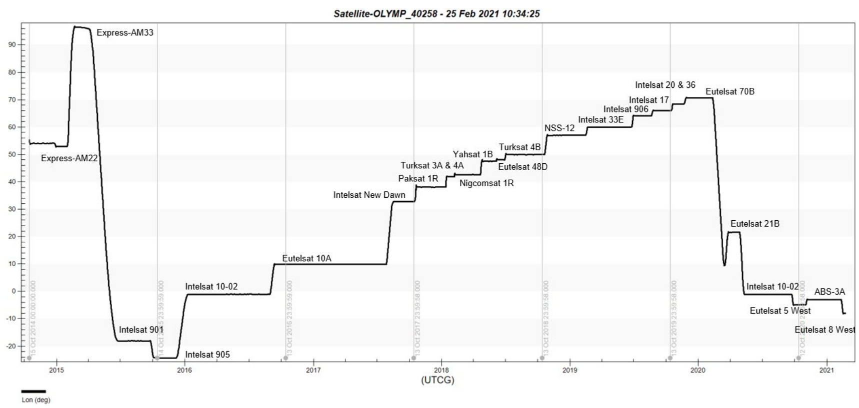
[207] Jonathan McDowell (@planet4589), "OK, let's talk about this story about Luch-Olimp passing "too closely" to the French-Italian military communications satellite ATHENA-FIDUS," Twitter thread, September 7, 2018, https://twitter.com/planet4589/status/1038147610073341953.

[208] Bob Hall, "Luch Space Activities," AGI web series, Ep. 14, June 26, 2019, https://youtu.be/D67dg9P3eDY.

[209] Bart Hendrickx," Project Numizmat," NASASpaceflightForums.com, April 9, 2020, https://forum.nasaspaceflight.com/index.php?topic=47851.new#new.

[210] T. Thayaparan and C. Wernik, "Noise Radar Technology Basics," Defence Research and Development Canada, December 2006, https://cradpdf.drdc-rddc.gc.ca/PDFS/unc55/p526766.pdf.

FIGURE 07: LUCH ORBITAL HISTORY



A compilation of Luch's orbital history and satellites visited. Credit: COMSPOC Corporation.

POTENTIAL MILITARY UTILITY

The most likely military utility for the Cosmos 2499, Cosmos 2504, Cosmos 2519, Cosmos 2535, Cosmos 2542, and Luch 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 and Cosmos 2504 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 3.1). Such inspection or surveillance could be used to support target identification and tracking for attack by other counterspace capabilities.

Luch'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 Luch eventually did. The evidence strongly suggests Luch 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 Luch 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 (See U.S. Co-Orbital ASAT, section 3.1) and the Chinese SJ-17 satellite (40258, 2014-058A) in 2017 (See Chinese Co-Orbital ASAT; section 1.1).

While the known on-orbit activities of Cosmos 2499, Luch, Cosmos 2504, Cosmos 2519, or Cosmos 2542 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. The RPO activities of Cosmos 2535 and Cosmos 2536 are more troubling, given the research papers linking them to deployment of aerosols or particulate clouds and the unexplained orbital debris generated by their RPO activities. Furthermore, the high-speed deployment of Cosmos 2523 from Cosmos 2521 and another object from Cosmos 2543 suggests they may be part of a ASAT interceptor deployment test, potentially linked to the Burevestnik program.

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 DA-ASAT operations, but likely not yet on a sufficient scale or at sufficient altitude to pose a critical threat to space assets. While Russia is actively testing what appears to be a new DA-ASAT capability in their Nudol system, it is not yet operational and does not appear 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:

01. **Nudol:** a rapidly maturing ground-launched ballistic missile designed to be capable of intercepting targets in LEO;
02. **Burevestnik:** an air-launched rocket that could either be a new version of the Kontakt DA-ASAT or a SLV to place co-orbital ASATs into LEO orbit, on a several-year development timeline; and
03. **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.

14A042 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.[211] The A-135 system included two missile interceptors, the exoatmospheric 51T6 (NATO designation "SH-11 Gorgon") and the endoatmospheric 53T6 (NATO designation "Gazelle"). While the system at the time possessed some dual-use potential for use as an ASAT, it was sharply limited and has likely since been eliminated by the retirement of the 51T6.[212]

Designs for the would-be replacement, the A-235 missile defense system (under the Russian codename Samolyot-M), first surfaced in 1985-1986, though little came of it at the time.[213] The system includes the 53T6M, an upgraded version of the Gazelle, as its short-range interceptor.

In August 2009, the PVO (Russian space defense company) Almaz-Antey signed a contract with the Russian Ministry of Defense, followed by subcontracts with OKB Novator and KB Tochmash (also known as the Nudelman Design Bureau) to work on a separate program called Nudol (U.S. designation PL-19).[214] KB Tochmash had previously developed a cannon for the Almaz military space station and worked on several other Soviet-era counterspace programs and OKB Novator has a long history developing long-range anti-aircraft missiles. In 2010, 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.[215] Individual components were tested in 2012[216] and initial non-flight testing of the system as a whole was successfully conducted in 2013.[217] In 2013, a second contract was signed between the Ministry of Defense and Almaz-Antey that also includes the Moscow Institute of Thermal Technology, which specializes in long-range solid fuel ballistic missiles, as a subcontractor instead of OKB Novator.[218]

The implication is that there may be two separate missiles being developed for Nudol, one short-range version being developed OKB Novator and one long-range version developed by the Moscow Institute of Thermal Technology.

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

212 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, p. 26 (2011) https://www.jstor.org/stable/resrep11662

213 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.

214 Bart Hendrickx, "Re: Russia Tests Nudol ASAT System," posting on the NASASpaceflight.com forum, January 18, 2020, https://forum.nasaspaceflight.com/index.php?topic=38943.msg2036403#msg2036403.

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

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

217 GSKB Annual Report 2013.

218 Bart Hendrickx, "Re: Russia Tests Nudol ASAT System," posting on the NASASpaceflight.com forum, January 18, 2020, https://forum.nasaspaceflight.com/index.php?topic=38943.msg2036403#msg2036403.

The evidence suggests Nudol is 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.[219] 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 significantly, 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].”[220] The system appears to be designated the 14Ts033 (14Ц033), comprised of the 14A042 Nudol rocket, 14P078 command and control system, and 14TS031 radar.[221]

There have been ten known flight tests of Nudol, eight of which were likely successful, and one additional unconfirmed test. Sources suggest that at least the November 2015 test was of just a rocket and did not include a kill vehicle.[222] 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.[223] Evidence is inconclusive as to whether any of the remaining tests included a kill vehicle.[224] Russia issued safety notices for airspace closures in June and November 2019 that are consistent with additional Nudol tests, but it appears the June test did not happen.[225] Two additional successful tests occurred on April 15, 2020, and December 16, 2020, with the USSPACECOM issuing statements confirming both test and calling them “further proof of Russia’s hypocritical advocacy of outer space arms control proposals designed to restrict the capabilities of the United States while clearly having no intention of halting their counterspace weapons programs.”[226,227] Table 6 to the right lists the known and suspected tests of the Nudol.

[219] “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,” Washington Free Beacon, December 2, 2015, http://freebeacon.com/national-security/russia-conducts-successful-flight-test-of-anti-satellite-missile/.

[220] 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.

[221] 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.

[222] 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.

[223] 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/.

[224] 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,” Washington Times, December 21, 2016, http://www.washingtontimes.com/news/2016/dec/21/russia-tests-anti-satellite-weapon-pl-19-nudol/.

[225] Pavel Podvig, “Nudol ASAT system tested from Plesetsk,” Russian Strategic Nuclear Forces, December 16, 2020, http://russianforces.org/blog/2020/12/nudol_asat_system_tested_from.shtml.

[226] USSPACECOM Public Affairs, “Russia tests direct-ascent anti-satellite missile,” United States Space Command, April 15, 2020, https://www.spacecom.mil/MEDIA/NEWS-ARTICLES/Article/2151611/russia-tests-direct-ascent-anti-satellite-missile/.

[227] USSPACECOM Public Affairs, “Russia tests direct-ascent anti-satellite missile,” United States Space Command, December 16, 2020, https://www.spacecom.mil/News/Article-Display/Article/2448334/russia-tests-direct-ascent-anti-satellite-missile/.

TABLE 06 - NUDOL FLIGHT TESTS TO DATE

DATE	SYSTEM	LAUNCH SITE	PAYLOAD	APOGEE	NOTES
Aug. 12, 2014[228]	Nudol	??	?	X	Failed shortly after launch
Apr. 22, 2015[229]	Nudol	??	?	X	Failed at launch
Nov. 18, 2015[230]	Nudol	Plesetsk[231]	KKV	200 km?	First successful test of missile
May 25, 2016[232]	Nudol	Plesetsk	??	100 km?	
Dec. 16, 2016[233]	Nudol	"Central Russia" (Plesetsk? Kapustin Yar?)	Likely KKV	100 km?	
Mar. 26, 2018	Nudol	Plesetsk	Likely KKV	?	First test from a mobile launcher
Dec. 23, 2018[234]	Nudol	Plesetsk	Likely KKV	?	
Nov. 15, 2019	Nudol	Plesetsk	Likely KKV	?	
Apr. 15, 2020	Nudol	Plesetsk	Likely KKV	?	
Dec. 16, 2020	Nudol	Plesetsk	Likely KKV	?	

Little is known for sure about the operational capabilities of the Nudol, and available estimates for maximum altitude vary widely from approximately 50 km[235] to nearly 1,000 km.[236] 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.[237] Russian media reports of the April 2015 failure suggested a rocket mass of 9.6 metric tons, which if true would indicate only a very limited ASAT capability.[238] The designation 14A is usually reserved for "space rockets" and intended for intercepting space objects, either satellites or nuclear warheads.[239]

228 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.

229 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.

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

231 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.

232 Gertz, Bill, "Russia Flight Tests Anti-Satellite Missile," 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.

233 Ibid.

234 Pavel Podvig, "Nudol ASAT was tested from Plesetsk in December 2018," Russian Strategic Nuclear Forces, February 6, 2019, http://russianforces.org/blog/2019/02/nudol_asat_was_tested_from_ple.shtml.

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

236 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/.

237 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.

238 Bart Hendrickx, "Re: Russia Tests Nudol ASAT System," posting on the NASASpaceflight.com forum, January 18, 2020, https://forum.nasaspaceflight.com/index.php?topic=38943.msg2036403#msg2036403

239 Ibid.

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

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

242 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.

243 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.

244 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.

FIGURE 08 - TEL-MOUNTED NUDOL

Artist's depiction from company calendar. Image credit: Almaz-Antey.[240]

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.[241] 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 territory.[242] 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.[243]

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 that appear to be environmental control systems (ECS) on the missile tubes—a feature typically associated with nuclear-armed missiles.[244]

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.[245] 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).[246] 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.[247] Moreover, Russian-language media reported in early 2018 that the system would not be equipped with nuclear warheads.[248] Deployment is reportedly scheduled for late 2018.[249]

Russian news media also reported that a new type of interceptor launched from a mobile vehicle was tested in July 2018 by the Russian Aerospace Forces. According to Andrey Prikhodko, deputy commander of air and missile defense of the Aerospace Forces, "After a series of trials, the interceptor missile confirmed its specifications and successfully performed its task, hitting the simulated target with the specified precision."[250] The specifics of the test were not released.

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.[251] 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".[252]

245 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/2019-09/a-history-of-ASAT-programs_lo-res.pdf

246 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.

247 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.

248 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.

249 "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

250 Bill Gertz, "Russian ASAT Test?" Washington Times, September 5, 2018, https://www.washingtontimes.com/news/2018/sep/5/russias-nudol-anti-satellite-missile-test/.

251 "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, https://www.globalsecurity.org/space/world/russia/mini.htm

252 Ibid.

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.[253] The system was also intended to be capable of deploying with little or no warning, in contrast to the USSR's co-orbital interceptors,[254] 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.[255]

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.[256] Whether such testing ever actually occurred is 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 the U.S. from discovering the program.[257] 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.[258] 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.[259] 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.[260] 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.[261] 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-announced Kinzhal air-launched cruise missile.[262] If so, that may indicate they are no longer slated for use with ASAT weapons.

253 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.

254 John Pike, "USSR/CIS Miniature ASAT," GlobalSecurity.org, updated October 4, 2016, http://www.globalsecurity.org/space/world/russia/mini.htm.

255 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.

256 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.

257 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.

258 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.

259 John Pike, "USSR/CIS Miniature ASAT," GlobalSecurity.org, updated October 4, 2016, http://www.globalsecurity.org/space/world/russia/mini.htm.

260 John Pike, "MiG-31BM (Bolshaya Modernizatsiya - Big Modernization)," GlobalSecurity.org, updated November 4, 2015, http://www.globalsecurity.org/military/world/russia/mig-31bm.htm.

261 Ibid.

262 John Pike, "USSR/CIS Miniature ASAT," GlobalSecurity.org, updated October 4, 2016, http://www.globalsecurity.org/space/world/russia/mini.htm.

Meanwhile, the integrated detection, targeting, tracking, and communications networks on which an airborne DA-ASAT system would depend are expanding and new facilities constructed: a new Krona ground radar-optical complex was recently constructed at Nakhodka (See Russian space surveillance complexes; page 10-20), 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.[263] 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."[264] 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."[265]

It is possible that Russia is working to bring the Kontakt capability online in the near future.[266] 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...."[267] 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.[268] 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.[269] Images of a MiG-31 carrying what was reportedly a mock-up of a new ASAT missile to replace the Kontakt appeared online in mid-September 2018.[270] Three anonymous U.S. government sources stated that the system was being actively tested with the goal of reaching operational readiness in 2022.[271]

263 "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.

264 "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.

265 Anatoly Zak, "Russian Anti-Satellite Systems," Russian Space Web, updated November 30, 2017, http://www.russianspaceweb.com/naryad.html.

266 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.

267 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.

268 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.

269 Ibid.

270 Tyler Rogoway and Ivan Voukadinov, "Exclusive: Russian MiG-31 Foxhound carrying huge mystery missile emerges near Moscow," TheDrive.com, September 29, 2018, http://thedrive.com/the-war-zone/23936/exclusive-russian-mig-31-foxhound-carrying-huge-mystery-missile-emerges-near-moscow.

271 Amanda Macias, "A never-before-seen Russian missile is identified as an anti-satellite weapon and will be ready for warfare by 2022," CNBC.com, October 25, 2018, https://www.cnbc.com/2018/10/25/russian-missile-identified-as-anti-satellite-weapon-ready-by-2022.html.

Information uncovered in spring 2020 suggests that the recent MiG-31B activity is linked to the Burevestnik co-orbital ASAT system, as opposed to a renewed version of the Kontakt DA-ASAT. Researcher Bart Hendrickx uncovered significant documentation for a three-stage solid rocket carried by a MiG-31B that would likely be used as a quick-response launch system to place one or more co-orbital ASATs into orbit (see "Recent Rendezvous and Proximity Operations in LEO" on page 2-6).[272] Construction work is on-going at Plesetsk airport to build infrastructure for future Burevestnik launches from aircraft-carried booster.[273]

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.[274] 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.[275] 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.[276] 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,[277] but had not yet completed testing.[278] Russian media reported 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.[279] 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;[280] Russia reportedly planned to field ten battalions of the new system at latest estimate.[281]

In June 2020, General Sergei Surovikin, Commander of the Russian Aerospace Forces, gave a lengthy interview in which he called the S-500 a "first generation space defense system" and noted that it will be capable of defeating low-orbit satellites and space strike systems in the future.[282]

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 of warning time before impact. Moreover, the potential for an air-launched DA-ASAT capability could dramatically expand the potential launch opportunities.

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, although it is possible given their advanced rocket and guidance technology.

[272] Bart Hendrickx, "Burevestnik: a Russian air-launched anti-satellite system," The Space Review, April 27, 2020, https://www.thespacereview.com/article/3931/1.

[273] Bart Hendrickx, posting on NASASpaceflightforum.com, July 28, 2020, https://forum.nasaspaceflight.com/index.php?topic=45734.msg2112384#msg2112384

[274] 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.

[275] 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," Washington Free Beacon, January 30, 2018, http://freebeacon.com/national-security/pentagon-china-russia-soon-capable-destroying-u-s-satellites/.

[276] Anatoly Zak, "Russian Anti-Satellite Systems," Russian Space Web, updated November 30, 2017, http://www.russianspaceweb.com/naryad.html.

[277] 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/.

[278] Ibid.

[279] 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.

[280] Ibid.

[281] Andrius Genys, "S-500," Military Today, April 5, 2017, http://www.military-today.com/missiles/s500.htm.

[282] "Чтобы господство в воздухе оставалось за нами," Redstar.ru, July 2, 2020, http://redstar.ru/chtoby-gospodstvo-v-vozduhe-ostavalos-za-nami/.

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 to 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 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, as well as use in Russia for protecting strategic locations and VIPs. New evidence suggests Russia may be developing high-powered space-based EW platforms to augment its existing ground-based platforms.

SPECIFICS

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.[283]

Some additional information on Russian EW doctrine, organization, and capabilities can be found in the report "Russia's Electronic Warfare Capabilities to 2025", published by the International Centre for Defence and Security in Estonia.[284]

283 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/.

284 Roger N. McDermott, "Russia's Electronic Warfare Capabilities to 2025," International Centre for Defence and Security, September 2017, https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf.

GNSS JAMMING

GNSS jamming, particularly of the U.S. GPS network, is a well-known technology and jammers are widely proliferated throughout the globe. Russia is assessed to be proficient in GPS jamming capabilities, having developed both fixed and mobile systems. The known systems are downlink 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.[285] 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.[286]

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.[287] 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”.[288, 289] 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.[290, 291, 292]

285 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.

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

287 “Electronic Warfare Chief Interviewed,” Russian Defense Policy, May 30 2017, https://russiandefpolicy.blog/tag/electronic-warfare/.

288 “R330ZH,” Rosobornexport, accessed March 15, 2018, http://roe.ru/eng/catalog/air-defence-systems/elint-and-ew-equipment/r-33ozh/.

289 “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/.

290 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.

291 “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/.

292 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 09 - RUSSIAN COUNTERSPACE EW SYSTEMS

Russian mobile counterspace EW systems deployed in Eastern Ukraine. Image credit: OSCE[293]

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.[294] In November 2018, there were media reports of widespread jamming of civil GPS signals in Norway and Finland at the same time as a major North Atlantic Treaty Organization (NATO) exercise.[295] The jamming reportedly affected military systems as well as civilian airliners, cars, trucks, ships, and smartphones. In March 2019, the Norwegian government claimed they had proof that the disruption was caused by Russian interference and demanded an explanation.[296]

In March 2019, the non-profit C4ADS published an in-depth report on Russian GNSS jamming and spoofing in Russia, Crimea, and Syria.[297] The report details nearly 10,000 suspected incidents across the entire Russian Federation, its occupied territories (including Crimea), and

293 Ukrainian Mission to OSCE & UN in Vienna (@UKRinOSCE), "Російські новітні системи озброєння - автоматизована станція перешкод Р-330 "Житель" та комплекс радіоелектронної боротьби "Тірада-2", зафіксовані Спеціальною моніторинговою місією ОБСЄ неподалік від н.п. Южна Ломуватка, на окупованій Росією частині Донбасу," Twitter.com, April 3, 2019, https://twitter.com/UKRinOSCE/status/1113385017185640448?s=20. Further analysis suggests that the system identified in the photo as a Tirada-2 was another EW system, the R-934BMV counter-UAV system. See Michael Sheldon, "Tirada-2 Likely Not Spotted in Ukraine," Digital Forensic Research Lab, July 17, 2019, https://medium.com/dfrlab/tirada-2-likely-not-spotted-in-ukraine-a4bb86956adc.

294 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.

295 "Norway, Finland suspect Russia of jamming GPS," GPS World, November 12, 2018, https://www.gpsworld.com/norway-finland-suspect-russia-of-jamming-gps/.

296 Nerijus Adomaitis, "Norway says it proved Russian GPS interference during NATO exercises," Reuters, March 18, 2019, https://www.reuters.com/article/us-norway-defence-russia/norway-says-it-proved-russian-gps-interference-during-nato-exercises-idUSKCN1QZ1WN.

297 "Above Us, Only Stars," C4ADS, March 2019, https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5c99488beb39314c45e782da/1553549492554/Above+Us+Only+Stars.pdf

overseas military facilities (primarily in Syria). In particular, the report tracks the use of GNSS spoofing as part of very important person (VIP) protection, protection of important strategic facilities, and airspace denial in active combat zones. The report was based on data from maritime AIS, ride sharing services such as Uber, and GPS-enabled fitness tracker applications. The spoofing often manifested in devices reporting they were located at one or more nearby airports, which may be an attempt to use the mandatory geofencing in commercial drones to deny their use. At Russian airbases in Syria, where weaponized drone attacks have occurred, military electronic warfare systems have reportedly been used to spoof GNSS and force attacking drones to land in designated spots.[298] The spoofing began in 2016, peaked in 2017, and appears to have lessened since being publicly reported.

In June 2019, Ben Gurion International Airport in Tel Aviv, Israel, experienced GPS disruptions that Israel attributed to Russian military activities. The International Federation of Airline Pilots' Associations noted that it had received multiple reports from pilots about loss of GPS signals near the airport.[299] The disruptions affected only airborne systems and not terrestrial navigation systems and only occurred during daytime. Israeli security officials stated that the disruptions were caused by defensive electronic warfare measures being taken at the Khmeimim Air Base in Syria, 390 km north, where Russian aircraft were based.[300]

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

In 2021, new research emerged about a Russian program called Tobol that appears to be aimed at protecting Russian satellites from uplink jamming.[301] The head of the project is linked to several academic papers and patents related to monitoring authentic satellite signals, detecting any focused interference, and transmitting additional signals to counter the interference.

JAMMING OF COMMUNICATIONS SATELLITES

Russia has dedicated capabilities for both downlink and uplink jamming of signals from communications satellites. The R-330Zh "Zhitel" mobile jammer is reportedly able to jam commercial INMARSAT and Iridium receivers within a tactical local area and has been deployed throughout recent Russian military campaigns.[302]

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."[303] The Tirada-2 reportedly can be used to conduct uplink jamming of communications satellites, potentially even capable of causing

298 "Head of the Russian General Staff's Office for UAV Development Major General Alexander Novikov holds briefing for domestic and foreign reporters," Ministry of Defence of the Russian Federation, January 11, 2018, http://eng.mil.ru/en/news_page/country/more.htm?id=12157872@egNews.

299 "Loss of GPS Signal at Ben Gurion Airport, Tel Aviv, Israel, (LLBG)," The International Federation of Airline Pilots' Associations, 19SAB05, June 25, 2019, https://www.ifalpa.org/media/3388/19sab05-loss-of-gps-signal-at-ben-gurion.pdf

300 "Ben Gurion Airport GPS Disruption Blamed on Russian Electronic Warfare," DefenseWorld,net, June 28, 2019, https://www.defenseworld.net/news/25041/Ben_Gurion_Airport_GPS_Disruption_Blamed_on_Russian_Electronic_Warfare.

301 Bart Hendrickx, "Russia gears up for electronic warfare in space (part 2)," The Space Review, November 2, 2020, https://www.thespacereview.com/article/4060/1.

302 Roger N. McDermott, "Russia's Electronic Warfare Capabilities to 2025," International Centre for Defence and Security, September 2017, https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf.

303 Anatoly Zak, "Russian Anti-Satellite Systems," Russian Space Web, November 30, 2017, http://www.russianspaceweb.com/naryad.html.

permanent damage.[304] The Russian Ministry of Defense has publicly stated that the Tirada-2 would enter service in 2019 and three additional versions were in development.[305] Another system reportedly in development is the Bylina-MM, which is designed to "suppress the on-board transponders of the millimeter band communications satellites Milstar, GBS, Skynet, Sicral, Italsat and Sakura" and may be linked to a much larger EW program also under the name Bylina.[306]

In September 2018, the Sputnik News service published a report claiming that Russia was developing a new electronic warfare aircraft that could be used to target satellite services.[307] The project is aimed at replacing the IL-22PP Porubshchik electronic warfare aircraft, which has become difficult to support due to its underlying airframe. The new project is reported to add the ability to interfere with space systems as well as air, ground, and maritime systems, but this has not yet been confirmed, nor has the specific capability of the system.

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 and has a reported effective range of 300 km.[308] Due to its range and power, it is also reported to be effective against LEO synthetic aperture radar imaging satellites.[309] Recent news reports have discussed delivery of a new EW system called Divnomorye that is meant to replace the Krashukha and serve as an integrated electronic warfare system against air, space, and ground systems.[310]

FIGURE 10 - KRASUKHA-4

A Russian mobile electronic warfare system used to jam radar. Image credit: Sputnik News.[311]

[304] Bart Hendrickx, "Russia gears up for electronic warfare in space (part 1)," The Space Review, October 26, 2020, https://www.thespacereview.com/article/4056/1.

[305] Ibid.

[306] Ibid.

[307] "Warfare Plane," Sputnik News, September 7, 2019, https://sputniknews.com/military/201807091066176858-russia-electronic-warfare-plane-satellites/

[308] E. Dilipraj, "Electronic Warfare: Russia's Capabilities," Centre for Air Power Studies, January 2016, pp.30-32, https://www.researchgate.netpublication/333420461_Electronic_Warfare_Russia's_Enhanced_Capabilities.

[309] "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/.

[310] Roger McDermott, "Russia's Electronic Warfare Capability: Training and Procurement," Eurasia Daily Monitor, May 17, 2018, https://jamestown.org/program/russias-electronic-warfare-capability-training-and-procurement/

[311] Bart Hendrickx, "Russia gears up for electronic warfare in space (part 1)," The Space Review, October 26, 2020, https://www.thespacereview.com/article/4056/1.

SPACE-BASED JAMMING

In October 2019, new research emerged that suggests Russia might be developing a new generation of nuclear reactors to power on-orbit jammers. Research done by Bart Hendrickx uncovered evidence of a project called Ekipazh that involves a Russian company, KB Arsenal, with a long history of developing nuclear reactors for satellites.[312] The Ekipazh project began on August 13, 2014, under the project code 14F350 and uses language that implies a connection to a "transport and energy module" (TEM) that had been previously proposed as part of the Plazma-2010 nuclear-powered space tug (a project that was apparently never funded).

While the exact payload for the Ekipazh program is unknown, KB Arsenal had previously suggested that the Plazma-2010 could be used to power space-based electronic warfare payloads.[313] KB Arsenal has argued that the nuclear reactor would be powerful enough to support jammers operating on on wide range of frequencies and interfering with electronic systems over a wide area from highly elliptical or geostationary orbits. Developing and deploying such a system would be consistent with Russia's stated military doctrine for space, but there is currently no public evidence of plans for operational deployment.

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.

However, conducting operationally-useful, dependable, and reliable jamming of highly-used military space capabilities, such as GNSS, is more difficult than most commentators suggest. Military GNSS signals are much more resilient to jamming than civil GNSS signals, and a wide variety of tactics, techniques, and procedures exist to mitigate attacks.[314] It is much more likely that an EW counterspace weapon would degrade military space capabilities rather than completely deny them.

312 Bart Hendrickx, "Ekipazh: Russia's Top-Secret Nuclear-Powered Satellite," The Space Review, October 7, 2019, https://www.thespacereview.com/article/3809/1

313 Ibid.

314 Brandon Davenport and Rich Ganske, "Recalculating Route: A Realistic Risk Assessment for GPS," War on the Rocks, March 11, 2019, https://warontherocks.com/2019/03/recalculating-route-a-realistic-risk-assessment-for-gps/.

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 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.

SPECIFICS

Russia 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.[315] With the economic 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.[316] 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 Japanese satellite in orbit. Work on the project was halted in 2011, due to lack of funding.[317]

In 2012, the Ministry of Defense announced the revival of the program.[318] 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.'"[319] The new system, called Sokol-Echelon ("Falcon Echelon"), will be equipped

315 John Pike, "Lasers," GlobalSecurity.Org, updated October 4, 2016, https://www.globalsecurity.org/space/world/russia/lasers.htm.

316 "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.

317 John Pike, "A-60 1A Airborne Laser," GlobalSecurity.org, August 3, 2018, https://www.globalsecurity.org/military/world/russia/a-60.htm.

318 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.

319 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 разрабатываетсяпротивоспутниковая система РЭБ," Ria Novosti, April 25, 2017, https://topwar.ru/114285-v-rf-razrabatyvaetsya-protivosputnikovaya-sistema-reb.html.

with the 1LK222 laser system, apparently a different system than the original Carbon Dioxide laser type from the 1980s. The new laser reportedly was to be fitted aboard a "brand-new, as-yet-unnamed" aircraft, according to Russian media reports,[313] which turns out to be a modified IL-76MD-90A transport.[314]

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. The program's chief designer, Aleksandr Ignatyev, stated in interviews in 2010 and 2014 that the program was initiated in response to the U.S. withdrawal from the Anti-Ballistic Missile Treaty in 2002 and was designed to "counter air-based and space-based reconnaissance assets in the infrared part of the spectrum."[315] 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 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.

The Beriev A-60 flew several flight tests during the 2010s with the goal of detecting and tracking satellites and aiming laser beams at them. Reportedly, one of the tests was directed at a Japanese satellite called Ajisaj. The program was reportedly near cancellation after that but survived and a new IL-76MD-90A aircraft is in the process of being outfitted with a laser.

PERESVET MOBILE LASER DAZZLER

Russia is also developing an advanced mobile laser dazzling system known as Peresvet that appears to be designed to protect mobile ICBMs from being imaged.[316] The system was formally named in part of a speech by Russian President Vladimir Putin on March 1, 2018, where he boasted about Russia's progress in arming their troops with laser weapons. President Putin called for a public contest to name the system, resulting in "Peresvet", which translates to "overexposure".[317] In July 2018, the Russian Ministry of Defense released a second video showing the shelters for the Peresvet vehicles and the training facility for the operators. The shelters are located alongside garrisons near Teykovo, Yoshkar-Ola, and Novosbirsk for the new Topol-MR ICBM currently being deployed.

320 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/.

321 Bart Hendrickx, posting on the NASASpaceflight.com forums, February 6, 2020, https://forum.nasaspaceflight.com/index.php?topic=50072.msg2042842#msg2042842 .

322 Bart Hendrickx, "Peresvet: a Russian mobile laser system to dazzle enemy satellites," The Space Review, June 15, 2020, https://www.thespacereview.com/article/3967/1.

323 Bart Hendrickx, "Peresvet: a Russian mobile laser system to dazzle enemy satellites," The Space Review, June 15, 2020, https://www.thespacereview.com/article/3967/1.

324 Ibid.

FIGURE 11 - THE PERESVET LASER SYSTEM

A Russian mobile laser system used to dazzle aerial and space reconnaissance assets.
Image credit: Russian Ministry of Defense.[325]

The Peresvet system consists of a laser connected to a gimbaled mirror, all of which is mounted inside a truck-towed trailer. A statement by the Russian Ministry of Defense in December 2018 said that the system had entered "experimental combat duty" and could "efficiently counter any aerial attack and even fight satellites in orbit.[326] While the system is unlikely powerful enough to destroy space objects, it is likely capable of temporarily dazzling visible optics used by satellites. Additionally, the system is linked to two patents for a "mobile optical telescope" designed to monitor and clean up space debris. The Chief of the General Staff of Russia's Armed Forces Valeriy Gerasimov confirmed that Peresvet's task is to "conceal the movements" of mobile missile systems, suggesting that its job is to dazzle aerial and space reconnaissance systems tying to detect, image, or track Topol-MR deployments.

In June 2020, General Sergei Surovikin, Commander of the Russian Aerospace Forces, gave a lengthy interview in which he stated the Peresvet system was operational.[327]

KALINA UPGRADE TO KRONA GROUND-BASED ELECTRO-OPTICAL SYSTEM

There are indications that Russia may be upgrading its Krona optical space surveillance system in the North Caucasus with laser dazzling or blinding capabilities. The Krona complex has historically included ground-based radars and optical telescopes for tracking, identifying, and characterizing space objects. Lasers have long been used to support optical tracking of space objects by providing range-finding for precision tracking and creating artificial guide stars used in adaptive optics.

[325] Ibid.

[326] Ibid.

[327] Чтобы господство в воздухе оставалось за нами,", Redstar.ru, July 2, 2020, http://redstar.ru/chtoby-gospodstvo-v-vozduhe-ostavalos-za-nami/

Research by Bart Hendrickx discovered bank guarantees and reports suggesting a project code-named Kalina to upgrade the facilities at Krona to include "functional suppression of electro-optical systems of satellites," which is likely a euphemism for dazzling or partially blinding optical sensors of satellite systems.[328] The project appears to be led by the Scientific and Industrial Corporation "Precision Instrument Systems" (NPK SPP).

In May 2018, NPK SPP presented a proposal to the Russian Academy of Sciences to install a laser at the Titov Optical Laser Centre (AOLTs) in the Altai mountain range that would be able to deorbit small pieces of space debris through laser ablation.[329] The idea is similar to historical U.S. proposals such as Project Orion in the 1990s.[330] More recently, NASA Ames proposed a "LightForce" concept for a less powerful laser to deorbit small space debris through radiation pressure.[331] Although NASA ultimately passed on the proposal, it has been picked up by a private company, Electo Optic Systems, and is being developed with support from the Australian government.[332] It is unclear if the NPK SPP proposal for AOLTs will go forward, or if it is linked to the Kalina proposal.

SATELLITE LASER RANGING (SLR): POTENTIAL FOR LASER DAZZLING

Russia has nine stations that are part of the International Laser Ranging Service Satellite (ILRS) network.[333] 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).[334] 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.[335] 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.[336] 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.[337] The Skif-DM spacecraft was reportedly a test vehicle for a one 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 first flight of the Energia SLV, which was eventually abandoned together with the Buran space shuttle program.[338]

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

[328] Bart Hendrickx, "Russia develops co-orbital anti-satellite capability," Jane's Intelligence Review, September 27, 2018, https://www.janes.com/images/assets/463/83463/Russia_develops_co-orbital_anti-satellite_capability.pdf.

[329] Bart Hendrickx, "Kalina: A ground-based laser ASAT system?", NASAspaceflight.com, October 2, 2018, https://forum.nasaspaceflight.com/index.php?topic=46485.

[330] J.W. Campbell, "Project ORION: Orbital debris removal using ground-based sensors and lasers," National Aeronautics and Space Administration, Technical Memorandum 108522, October 1996, https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19960054373.pdf.

[331] Jahn Stupl et al, "LightForce Photon-pressure collision avoidance: Updated efficiency analysis utilizing a highly parallel simulation approach https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20150000244.pdf.

[332] Nick Grimm, "Scientists plan to use high powered lasers to track and shoot away space junk," Australian Broadcasting Corporation, March 21, 2018, https://www.abc.net.au/news/2018-03-21/scientists-plan-to-shoot-down-space-junk-with-a-laser/9573066.

[333] International Laser Ranging Service web page, List of Stations; online https://ilrs.cddis.eosdis.nasa.gov/network/stations/index.html.

[334] Yousaf Butt, "Effects of Chinese Laser Ranging on Imaging Satellites," Science and Global Security, 17:20-35, 2009, http://scienceandglobalsecurity.org/archive/sgs17butt.pdf

[335] 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.

[336] Ibid.

[337] "Polyus/Skif-DM," Buran-Energia.com, accessed March 16, 2018, http://www.buran-energia.com/polious/polious-desc.php.

[338] 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.

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

DEWs, primarily lasers, offer significant potential for military counterspace applications. They offer the possibility of interfering with or disabling a satellite without generating significant debris. The technologies required for ground-based lasers systems are well developed. Ground-based systems can dazzle or blind EO satellites, or even inflict thermal damage on most LEO satellites.

In contrast, the technical and financial challenges to space-based DEW for counterspace remain substantial. These include mass of the weapon, consumables and disturbance torques (chemical lasers), electrical power generation (solid state and fiber lasers, particle beams), target acquisition and tracking, and the potential required large size of constellation. The acquisition and tracking challenges are greatly simplified in a co-orbital GEO or LEO scenario.

However, both ground- and space-based DEW counterspace capabilities do have significant drawbacks in assessing their effectiveness. 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 a non-destructive DEW attack actually worked.

02

2.5 – RUSSIAN SPACE SITUATIONAL AWARENESS CAPABILITIES

ASSESSMENT

Russia has sophisticated SSA capabilities that are likely second only to the United States. Russian SSA capabilities date to the Cold War and leverage significant infrastructure originally developed for missile warning and missile defense. Although some of these capabilities atrophied after the fall of the Soviet Union, Russia has engaged in several modernization efforts since the early 2000s to reinvigorate them. While the government owned and operated SSA capabilities are limited to the geographic boundaries of the former Soviet Union, Russia is engaging in international civil and scientific cooperative efforts that likely give it access to data from SSA sensors around the globe. Today, Russia is able to maintain a catalog of Earth-orbiting space objects in LEO that is somewhat smaller than the United States but a slightly more robust catalog of HEO and GEO objects.

SPECIFICS

Like the United States, Russia developed its original SSA capabilities as part of the Cold War space and nuclear rivalry. The Russian Space Surveillance System (SSS) consists of multiple phased array radars that are primarily used for missile warning along with dedicated ground-based electro-optical telescopes. Several of the SSS sensors are located in former Soviet republics and are operated by Russia under a series of bilateral agreements with the host countries.

Russian ground-based radar tracking of space objects began as part of their anti-ballistic missile and ASAT efforts. The original Russian SSA radars were the 5N15 Dnestr (NATO codename HEN HOUSE) installations built in the 1960s near Irkutsk and Sary Shagan.[339] Each site had four complexes, with each complex containing a pair of Dnestr radars that could track LEO objects linked to a command and control building, and was intended to be the targeting system for the Soviet IV ASAT system (See Russian Co-Orbital ASAT; section 2.1).[340] Beginning in the 1970s, the radars were incrementally upgraded to Dnestr-M and integrated into the national ballistic missile early warning network, and most were later upgraded to the Dnepr variant. The Dnepr upgrades included new installations at Balkhash (modern day Kazakhstan); Mishelevka, Siberia; Skrunda (modern day Latvia), Olenegorsk, Kola Peninsula; Sevastapol, and Mukachevo (both in modern day Ukraine). The dissolution of the Soviet Union eventually led to the radars in Skrunda, Sevastapol, and Mukachevo to be shut down by the early 2000s.

In 2009, Russia began construction of the Voronezh phased array radar to replace the Dnestr-M and Dnepr radars for both ballistic missile early warning and SSA missions. The Voronezh-M uses very-high frequency (VHF) radio waves, Voronezh-DM uses UFH, and Voronezh-VP works in L-Band. The DM version is claimed to be able to detect objects the size of a soccer ball at 8,000 km and track up to 500 objects simultaneously. The first Voronezh was built at a new location in Lekhtusi near St. Petersburg and was operational in 2012.[341]

339 Sean O'Connor, "Soviet and Russian Space Surveillance Facilities," IMINT and Analysis, June 23, 2008, https://geimint.blogspot.com/2008/06/soviet-russian-space-surveillance.html

340 Ibid.

341 Pavel Podvig, "Radar in Lekhtusi Begins Combat Duty," Russian Strategic Nuclear Forces, February 11, 2012, http://russianforces.org/blog/2012/02/radar_in_lekhtusi_begins_comba.shtml

The remaining Dnepr radar sites are planned to be converted over to Voronezh by 2022, with several new sites also being developed.[342] As of 2019, twelve early warning radars were operational across 11 sites with four more radars under construction or planned. It is unclear if all of these sites are actively involved in providing SSA data.

FIGURE 12 - RUSSIAN MISSILE WARNING AND SSA RADARS[343]

Radar station	Radars	Status
Olenegorsk (RO-1)	Dnepr	operational
	Voronezh-VP?	under construction (2022)
Pechora (RO-30)	Daryal	operational
Vorkuta	Voronezh-VP, -SM	under construction (2021)
Mishelevka (OS-1)	Dnepr	operational
	2xVoronezh-VP	operational
Lekhtusi	Voronezh-M	operational
Lekhtusi/Ragozinka-2	Voronezh-SM	planned
Armavir	2xVoronezh-DM	operational
Kaliningrad	Voronezh-DM	operational
Barnaul	Voronezh-DM	operational
Yeniseysk	Voronezh-DM	operational
Orsk	Voronezh-M	operational
Sevastopol	Voronezh-SM	planned (2024)
Balkhash, Kazakhstan (OS-2)	Dnepr	operational
Baranovichi, Belarus	Volga	operational

Russia's primary optical SSA facility is the Okno ("Window") complex located near the city of Nurek in northern Tajikistan. The Okno facility consists of a cluster of ten electro-optical telescopes, laid out in two clusters of 4 and 6 telescopes each, that are designed to detect space objects at altitudes from 2,000 to 40,000 km, although some reports suggest an additional capability to track space objects down to 120 km and up to 50,000 km, as well as conduct TT&C with Russian civilian satellites.[344] Each telescope is covered by a 25-meter metal dome to protect it during the daytime. Although construction began in the 1980s, it was not commissioned until 2004 and underwent significant modernization that was completed in 2018. Originally, Western analysts suspected Okno was being built as a laser weapons site, but those speculations were proven wrong.[345] Originally, a total of four Okno sites were planned throughout the Soviet Union, but ultimately work was only started on one, Okno-S, in Primorsky Krai in the Russian Far East. However, open source analysts have yet to identify the site nor determine its status.

342 "Three Advanced Early Warning Radars Enter Service in Russia," TASS, December 19, 2017, https://tass.com/defense/981965

343 Pavel Podvig, "Early Warning," Russian Strategic Nuclear Forces, January 3, 2020, http://russianforces.org/sprn/.

344 Allen Thompson, "Sourcebook on the Okno, Okno-S, Krona, and Krona-N Space Surveillance Sites," Federation of American Scientists, Version 2014-11-19, pg 6 and pg 15, https://fas.org/spp/military/program/track/okno.pdf

345 William Broad, "Private Satellite Photos Offer Clues About Soviet Laser Site," New York Times, October 23, 1987, https://www.nytimes.com/1987/10/23/us/private-satellite-photos-offer-clues-about-soviet-laser-site.html.

Russia also operates the Krona radio-optical complex near Storozhevaya in southwestern Russia. Krona uses a combination of radar and optical sensors to track, image, and characterize space objects. The radar, located at 43°49'34"N, 41°20'35"E, includes both ultra-high frequency (UHF) and super-high frequency (SHF) transmitters and the optical sensor, located 30 km away at 43.7169171°N, 41.2316883°E, includes a laser locator and electro-optical imager.[346] The dual radar bands allow for both broad area search and detection and precise tracking. The precise tracking data is used to aim the laser, which then generates a precise lidar image of the object. Originally, four Krona complexes were planned but only one additional one, Krona-N, is under construction at 42°56'8.52"N 132°34'36.37"E, near Nakodka in the Russian Far East.[347]

The Altay Optical Laser Center, located near the small Siberian town of Savvushka, is a specialized facility for providing high resolution images of space objects.[348] The facility uses a laser rangefinder and a 60-centimeter telescope equipped with adaptive optics to enable high resolution images of satellites in LEO. A second 3.12-meter telescope is under construction that would allow an imaging resolution of 25 centimeters or better out to 1,000 kilometers.[349] In 2015, the site was reportedly used to image a U.S. LACROSSE radar reconnaissance satellite.[350] Russia is currently engaged in programs to upgrade many of its SSS sensors, although current status is difficult to judge from open sources. In 2016, Russian state media reported that upgrades were planned for four radio-electronic sensor complexes in the Altai Republic, the Far East, Crimea and the Republic of Buryatia.[351] Russia has also announced plans to set up new ground-based observatories in the Nenets Autonomous Region to monitor space objects in polar orbits.[352] In addition to the government owned and operated facilities, Russia also has a program to develop a network of scientific instruments for SSA purposes. The International Scientific Optical Network (ISON) is a collection of more than 38 observation facilities of various affiliation with 90 telescopes in 16 countries that are coordinated by the Keldysh Institute of Applied Mathematics (KIAM) of the Russian Academy of Sciences.[353] The telescopes are used to track space objects and orbital debris in Earth orbit as well as Near-Earth Objects (asteroids and comets) in orbit around the Sun. The ISON network includes four different types of partners: 26 telescopes used by KIAM for scientific research, 24 telescopes used by KIAM Ballistics Service for commercial purposes, 22 telescopes used by Roscosmos/TsNIIMash for conjunction analysis, and 18 telescopes used by the Vympel Corporation for SSA.[354] The network collects more than 2 million observations annually and maintains a catalog of more than 6,000 space objects in HEO or GEO orbits. In 2014, Vympel launched a public portal to access the catalog maintained by ISON.[355] In December 2019, KIAM announced a partnership with the United Nations Office of Outer Space Affairs to launch a project to provide small telescopes and training to select developing countries free of charge beginning in 2020.[356]

346 Allen Thompson, “Sourcebook on the Okno, Okno-S, Krona, and Krona-N Space Surveillance Sites,” Federation of American Scientists, Version 2014-11-19, https://fas.org/spp/military/program/track/okno.pdf/.

347 Ibid.

348 Allen Thomspon, “The Altay Optical-Laser Center Sourcebook,” Federation of American Scientists, updated March 29, 2011, https://fas.org/spp/military/program/track/altay.pdf.

349 Ibid, pg 3.

350 Steven Aftergood, “Russia Images the LACROSSE Spysat,” Secrecy News, April 23, 2015, https://fas.org/blogs/secrecy/2015/04/lacrosse-altay/.

351 “Russia to Deploy New Space Surveillance System Element to Four Regions,” Sputnik, November 30, 2016, https://www.defencetalk.com/russia.-to-deploy-new-space-surveillance-system-elements-in-four-regions-68624/.

352 Russia to Set Up SSA Observatories Along Arctic Ocean Coast,” SpaceWatch Global, November 2018, https://spacewatch.global/2018/11/russia-to-set-up-ssa-observatories-along-arctic-ocean-coast/.

353 I. Molotov, V. Voropaev, G. Borovin, and A. Romanov, “International Scientific Optical Network (ISON) for the Near-Earth Space Monitoring: the Latest Achievements and Prospects,” ISON, presentation to the fifty-fourth session of the Scientific and Technical Subcommittee of the United Nations Committee on the Peaceful Uses of Outer Space, January 30 – February 10, 2017, https://www.unoosa.org/documents/pdf/copuos/stsc/2017/tech-05E.pdf.

354 Ibid.

355 The public catalog can be accessed at http://spacedata.vimpel.ru/.

356 United Nations Office for Outer Space Affairs,“UNOOSA and the Keldysh Institute of Applied Mathematics are Working on an Announcement of Opportunity to Provide Telescopes to Institutions in Developing Countries,” SpaceRef, December 24, 2019, http://www.spaceref.com/news/viewpr.html?pid=55062.

SSA data is processed by two different centers, one military and one civil. The military center is the 821st Main Centre for Reconnaissance of Situation in Space (Главный центр разведки космической обстановки, tr. GTsRKO), located in the village of Dubrovo about 35 km outside of Moscow.[357] The Centre controls the SSS and uses its data products for both offensive and defensive counterspace applications. In 2016, a new civil SSA monitoring center called Automated Warning System on Hazardous Situations in Outer Space (ASPOS OKP) began operations under contract to Roscosmos,.[358] ASPOS OKP utilizes data from ISON and other Russian SSA assets to detect and track objects in Earth orbit above 2000 km and provide a range of SSA services, including conjunctions, fragmentations, re-entries, and post-mission disposal.

In May 2020, Roscosmos outlined plans for several upgrades to its SSA capabilities under a program called Milky Way.[359] In remarks to the TASS news agency, Alexander Bloshenko, Roscosmos Executive Director for Long-Term Programmes and Science, said that Russia would develop at least one space surveillance satellite and space surveillance hosted payloads on future Sfera-class Earth observation satellites, and a hosted payload on the International Space Situation (ISS), to complement its existing ground-based telescope network.[360] Bloshenko stated that these upgrades, along with machine learning, would allow Russia to better identify orbital debris and reduce uncertainty in calculating collision hazards in LEO.

Russia also has several institutions involved in space weather research. Russia operates a network of ground stations that cover 170 degrees of longitude and 60 degrees of latitude to measure various geomagnetic and space weather effects.[361] Russia also operates multiple satellites with on-orbit space weather sensors, including the Meteor series of polar-orbiting meteorological satellites. Space weather predictions and warnings are provided by the Federal Service for Hydrometeorology and Environmental Monitoring.[362] The Institute for Applied Geophysics contributes to the ISES.

MILITARY UTILITY

Russia possesses sophisticated SSA capabilities that allow it to track, identify, and characterize nearly all objects bigger than 10 centimeters in Earth orbit. While the Russian SSS possess many of the same shortcomings of the U.S. SSN in geographic coverage of LEO due to its northern location, the addition of the ISON network eliminates those shortcomings for GEOs. Russian SSA capabilities were originally developed as part of their ASAT capabilities and likely maintain the ability to effectively detect, track, characterize, and target many adversary national security satellites. The on-going modernization of Russia's SSA capabilities, combined with the modernization of their offensive counterspace capabilities, suggest a focus on developing an integrated operational system for future conflicts that extend into space.

357 "Главный центр разведки космической обстановки отметил свое 25-летие," Topwar.ru, July 11, 2013, https://topwar.ru/30674-glavnyy-centr-razvedki-kosmicheskoy-obstanovki-otmetil-svoe-25-letie.html.

358 V. Agapov, "The use of ASPOS OKP System in the Interests of Ensuring the Safety of Space Operations and Increasing Awareness About the Situation in High Orbits," presentation to the sixty-first session of the United Nations Committee on the Peaceful Uses of Outer Space, June 25, 2018, http://unoosa.org/documents/pdf/copuos/2018/copuos2018tech05E.pdf.

359 "Russia to develop space surveillance satellite to monitor space debris as part of Milky Way SSA network," SpaceWatch Global, June 2020, https://spacewatch.global/2020/06/russia-to-develop-space-surveillance-satellite-to-monitor-space-debris-as-part-of-milky-way-ssa-network/

360 "Russia to launch first satellite to monitor space junk in 2027," TASS, May 28, 2020, https://tass.com/science/1161437

361 S. Avdyushin et al, "Russian Space Weather Initiatives," ResearchGate, January 1999, https://www.researchgate.netpublication/237384438_RUSSIAN_SPACE_WEATHER_INITIATIVES.

362 "Space Weather Today and Possible Effects," Federal Service for Hydrometeorology and Environmental Monitoring, accessed February 21, 2020, http://space-weather.ru/

2.6 – RUSSIAN COUNTERSPACE POLICY, DOCTRINE, AND ORGANIZATION

ASSESSMENT

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. Russia has recently re-organized its military space forces into a new organization that combines space, air defense, and missile defense capabilities. Although technical challenges remain, the Russian leadership has indicated that Russia will continue to seek parity with the United States in space.

SPECIFICS

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.[363] 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.[364]

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.[365]

363 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.

364 Anton Lavrov, "Russia's GLONASS Satellite Constellation," Moscow Defense Brief, no. 4 (2017), http://www.mdb.cast.ru/mdb/4-2017/item2/article3/.

365 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.

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. 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 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.[366]

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.[367]

Since 2011, Russia has maintained the minimum 24 GLONASS satellites necessary for its military applications.[368] 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.[369] 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.[370] In Syria, Russian forces have used satellite-enabled weapons ranging from more accurate air-launched and dropped munitions to sea-based PGM employment.[371] Satellite navigation has also improved Russian situational awareness on the ground.[372]

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.[373] At the operational-strategic level, other systems would challenge western military forces use of satellite-based communications over large sections of the battlefield.[374] The Russian military is integrating these capabilities into all of its combat units down to the lowest level with an understanding that information warfare, to include space-based capabilities, is essential to winning in modern warfare.

[366] Yu Donskov, A.L. Moraresku, and V.V. Panasyuk, "On the Issue of Disorganization of Command and Control," Voennaia mysl, no. 8 (2017).

[367] Anton Lavrov, "Russia's GLONASS Satellite Constellation," Moscow Defense Brief, no. 4 (2017), http://www.mdb.cast.ru/mdb/4-2017/item2/article3/.

[368] Ibid.

[369] Constantine Bogdanov, "Russian Operations in Syria," Natsional'naia oborona, no. 12 (2017).

[370] Ibid.

[371] Dmitry Kornev, "Russian High-Precision Weapons in Syria," Moscow Defense Brief, no. 3 (2016), http://www.mdb.cast.ru/mdb/3-2016/item4/article1/.

[372] Anton Lavrov, "Russia's GLONASS Satellite Constellation," Moscow Defense Brief, no. 4 (2017), http://www.mdb.cast.ru/mdb/4-2017/item2/article3/.

[373] Roman Skomorokhov, "Станция постановки помех Р-330Ж «Житель»," accessed March 15, 2018, https://topwar.ru/98467-stanciya-postanovki-pomeh-r-330zh-zhitel.html.

[374] 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.

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, 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.[375] 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.[376]

Russian objectives in space, however, face significant challenges over the near term primarily from industry shortcomings.[377] 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.[378] Despite these challenges, Russian President Vladimir Putin recently announced a number of initiatives suggesting that Russia intends to aggressively address its shortfalls in space.[379]

SPACE AND COUNTERSPACE ORGANIZATION

Russian space activities are run by Roscosmos. Originally created in 1992 as the Federal Space Agency, it was dissolved in 2015 and its responsibilities transferred to the Roscosmos state corporation, which was also merged with the United Rocket and Space Corporation.[380] In its current form, Roscosmos is responsible for Russisan civil space activities as well as supervising companies manufacturing civil and military space, missile, and rocket hardware. Russia's space strategy is defined by the Ministry of Defense, although some suggest Roscosmos may have a role.[381] In 2015, Russia also reorganized its military space forces.From 2001 until 2011, Russian military space forces were a separate branch of the military. In 2011, they became part of the Aerospace Defense Troops and in 2015 the Aerospace Defense Troops were merged with the Air Force to become the Aerospace Forces. The new Aerospace Forces have authority for conducting space launches,

[375] “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,” 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.

[376] 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.

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

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

[379] “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.

[380] Avaneesh Pandey, “Russia's Federal Space Agency Dissolved, Responsibilities To Be Transferred To State Corporation,” International Business Times, December 28, 2015, https://www.ibtimes.com/russias-federal-space-agency-dissolved-responsibilities-be-transferred-state-2240831.

[381] Forian Vidal, “Russia’s Space Policy: The Path of Decline?”, Études de l’Ifri, Ifri, p.15, January 2021, https://www.ifri.org/sites/default/files/atoms/files/vidal_russia_space_policy_2021_.pdf.

maintaining ballistic missile early warning, the satellite control network, and the space surveillance network along with anti-air and anti-missile defense.[382] According to Russia Defense Minister Sergei Shoigu, the move was motivated by a recognition of a "shift in the combat 'center of gravity' toward the aerospace theater" and also a desire to counter U.S. capabilities such as the Prompt Global Strike Program.[383]

A report issued in 2017 noted that company-level EW units, including a platoon dedicated to operating the R-330Zh "Zhitel" counter-GPS and satellite communications jammer, are now included organically within each Russian Motorised Rifle Brigade.[384] Additionally, Russia maintains five dedicated EW brigades that can provide operational or strategic effects out to several hundred kilometers.[385]

The budget for Russian military space activities was estimated at USD 1.7 billion in 2020.[386]

382 Matthew Bodner, "Russian military merges Air Force and Space Command," The Moscow Times, August 3, 2015, https://www.themoscowtimescom/2015/08/03/russian-military-merges-air-force-and-space-command-a48710.

383 Ibid.

384 Roger N. McDermott, "Russia's Electronic Warfare Capabilities to 2025," International Centre for Defence and Security, September 2017, pp. 5-6, https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_ElectronicWarfare_to_2025.pdf

385 Ibid, pp. 7

386 Павел Лузин, "Цена и перспективы военной космической программы," Riddle, May 22, 2020, https://www.ridl.io/ru/cena-i-perspektivy-voennoj-kosmicheskoj-programmy/.

03 The United States

The United States currently has the most advanced 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 that uses electronic warfare capabilities to interfere with satellite signals, but it also has multiple other operational systems that could be used in counterspace roles. 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 United States has started a major reorganization of its military space capabilities under the leadership of its emerging Space Force.

The following sections summarize U.S. counterspace development across co-orbital, direct ascent, directed energy, electronic warfare, and space situational awareness 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 HTK 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.

PROJECT SAINT

Project SAINT (also known as the Satellite Inspector Program) was a USAF effort to develop a system that could be used initial as a satellite inspector but eventually could be turned into a co-orbital ASAT weapon. The concept began as a result of a set of studies done from 1956 through 1959 on ways to defend against hostile satellites.[387] Following those studies, the USAF developed initial ideas for three different concepts: one that was uncrewed and ground-launched, one that was uncrewed and air-launched, and a third that was crewed. In 1960, the USAF pressed forward with a "satellite inspector" version of the program in response to tough questions over an unidentified space object that was detected in December 1959 (that later turned out to be a piece of debris from the U.S. Discoverer V satellite).[388]

The inspector concept called for the SAINT vehicle to be launched into orbit on an Atlas booster, after which it would match orbits with the target and use on-board television cameras and radars to inspect the target from as close as 50 feet. However, the USAF also hoped that later version of the SAINT vehicle would include a kill mechanism, such as high-explosive rockets. The USAF planned for an initial set of four intercept tests beginning in 1963 and SAINT to be fully operational by the summer of 1967.[389] However, lack of budget support and political concerns led to the program's cancellation in 1962 before any on-orbit tests were conducted.

[387] Paul Stares, The Militarization of Space: U.S. Policy, 1945-1984, Cornell University Press, August 1, 1985, pp. 112.

[388] Ibid, pg. 112-113.

[389] Ibid, pg. 115.

DELTA 180

Although not explicitly designed as a co-orbital ASAT weapon, the United States did conduct a successful co-orbital 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.[390] 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 two objects (Delta 1 R/B, 1986-069B, 16938; USA 19, 1986-069A, 16937), presumably the D2 and PAS, respectively, 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.[391] 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 USAF, National Aeronautics and Space Administration (NASA), and Defense Advanced Research Projects Agency (DARPA) have all conducted tests and demonstrations of close approach and rendezvous technologies in LEO. On January 29, 2003, the USAF launched the XSS-10 (2003-005B, 27664) 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 (203-005C, 27665) conducted its passivation 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).[392] XSS-11 (2005-011A, 28636) was launched on April 11, 2005, and according to the official fact sheet, proceeded to "successfully demonstrate rendezvous and proximity operations with the expended rocket body [that placed it in orbit]."[393] The fact sheet also stated that over the following 12 to 18 months, the spacecraft "conduct[ed] rendezvous and proximity maneuvers with several USowned, dead or inactive resident space objects near its orbit." However, it is impossible to verify whether these activities occurred, and whether 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.

390 John Dassoulas and Michael D. Griffin, "The Creation of the Delta 180 Program and Its Follow-ons," Johns Hopkins APL Technical Digest, vol. 11, Numbers 1 and 2 (1990): p.86, https://www.jhuapl.edu/Content/techdigest/pdf/V11-N1-2/11-01-Dassoulas.pdf.

391 "VSE (Delta-180, DM-43)," Gunter's Space Page, accessed March 22, 2018, http://space.skyrocket.de/doc_sdat/vse.htm.

392 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.38pdf;jsessionid=906BB52FE69F848048883B704DB20F07.smart2?sequence=2.

393 "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.

394 Ibid, p.2

395 "Overview of the DART Mishap Investigation Results," NASA, accessed March 22, 2018, http://www.nasa.gov/pdf/148072main_DART_mishap_overview.pdf.

396 "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.

397 Stephen Clark, "In-space Satellite Servicing Tests Come to an End," SpaceFlight Now, July 4, 2007, http://spaceflightnow.com/news/n0707/04orbitalexpress/.

FIGURE 13 - MINOTAUR UPPER STAGE

Image taken by XSS-11 from a distance of approximately 500 m.
Image credit: AFRL.[394]

On April 15, 2005, NASA launched the DART satellite (2005-014A, 28642) to conduct an autonomous rendezvous experiment with a U.S. Navy communications satellite, the MUBLCOM satellite (1999-026B, 25736). 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.[395]

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 (2007-006A, 30772) and the NEXTSat client vehicle (2006-006C, 30774). 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 the next few months demonstrating multiple rendezvous and capture scenarios, including the first-ever use of a robotic arm to autonomously capture another space object.[396] The two spacecraft were deactivated in July 2007.[397]

FIGURE 14 - ORBITALEXPRESS MISSION PLAN

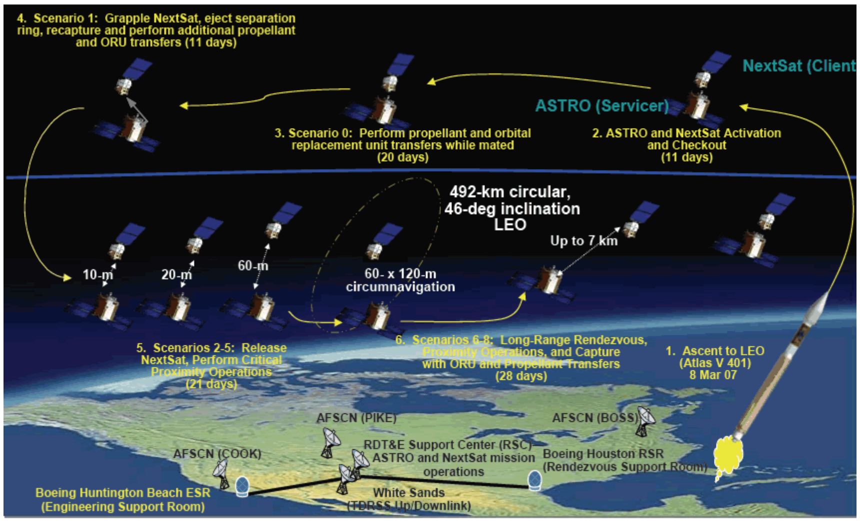


Image credit: Boeing.[398]

SECRET DEPLOYMENT OF SATELLITES

On October 27, 2019, the Orbital Test Vehicle 5 (OTV-5) flight of the X-37B completed a record-breaking 780-day stay in orbit with a landing at NASA's Kennedy Space Center Shuttle Landing Facility. In a press release, the director of the Rapid Capabilities Office stated that as part of its mission it had provided a ride for small satellites.[399] Although a similar reference was made during the launch of OTV-5 in September 2017, it was perceived at that time to small satellite ride shares that would be attached to the upper stage of the Falcon 9 booster that placed it into orbit, as has been done on previous launches. However, no such deployment was announced or cataloged by the U.S. military after the launch of OTV-5, leading to the conclusion that the deployment must have occurred from the X-37B itself later in the mission. On February 11, 2020, the U.S. military quietly cataloged three new satellites – USA 295 (45169, 2017-052C), USA 296 (45170, 2017-052D), and USA 297 (45171, 2017-052E) – associated with OTV-5. However, no orbital information was provided for those three satellites. On February 12, the catalog was updated to reflect that they were no longer in orbit. An analysis done by Dr. Marco Langbroek suggests the three cubesats had to be deployed before August 2018 if they were of 3U size.[400] The latest launch of the X-37B was OTV-6 (2020-029A, 45606) in May 2020, carrying for the first time a new service module at its end that would give it more room for payloads and experiments; one of them is a satellite, FalconSAT 8, built by students at the USAF Academy.[401] OTV-6 released a subsatellite, USA 300 (2020-029B, 45610), at the end of May 2020, which *could* be FalconSAT 8 but it has not been identified as such by the U.S. military.[402] OTV-6 also tested an on-orbit power beaming system, the U.S. Naval

[398] "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/.

[399] Secretary of the Air Force Public Affairs, "X-37B Breaks Record, Lands After 780 Days In Orbit," United States Air Force, October 27, 2019, https://www.af.mil/News/Article-Display/Article/1999734/x-37b-breaks-record-lands-after-780-days-in-orbit/.

[400] Marco Langbroek, "Launching Cubesats From the X-37B OTV 5: Lifetime Modelling With GMAT," SatTrackCam Leiden (b)log, February 21, 2020, https://sattrackcam.blogspotcom/2020/02/launching-cubesats-from-x-37b-otv-5.html

[401] Stephen Clark, "Upgraded X-37B spaceplane rockets into orbit aboard Atlas 5 launcher," Spaceflightnow.com, May 17, 2020, https://spaceflightnow.com/2020/05/17/upgraded-x-37b-spaceplane-rockets-into-orbit-aboard-atlas-5-launcher/.

[402] Jonathan McDowell, Tweet, May 30, 2020, https://twitter.com/planet4589/status/1266781929078231041.

Research Laboratory's (NRL) Photovoltaic Radio-frequency Antenna Module (PRAM), that collects solar power and transforms it into a microwave beam, which could then be sent to Earth and changed into energy that could run electrical devices; the PRAM could also potentially lead to capabilities that could provide offensive directed energy counterspace weapons.[403]

The mission of the X-37B has long been a source of mystery and speculation. While the USAF has acknowledged the existence of the X-37B program and announced launches and landings, it has been secretive about the mission of the X-37B and its location and activities while on orbit. Officially, the USAF has stated that the X-37B is a platform for testing new technologies and operational concepts.[404] However, the secrecy has led to a huge amount of speculation, particularly in Russia and China, that the X-37B is some sort of orbital bomber or secret weapons testing platform. Complicating things further is that the USSF's Space Delta 9 is now responsible for overseeing the X-37B's operations once it is in orbit. Space Delta 9 mission is to "protect and defend operations from space and provides response options to deter and defeat adversary threats in space."[405]

Analyzing the known facts about the size, shape, and orbit of the X-37B can provide a more useful answer. The spaceplane resembles the now-retired space shuttle orbiter in overall shape but is much smaller and completely robotic with a payload bay is roughly the size of a pickup truck bed.[406] This significantly limits its ability to host weapons, and its limited gliding capability makes it not militarily useful as a orbital bomber.[407] Based on tracking data from hobbyists, the X-37B normally orbits between 300 and 400 km and at inclinations between 38 and 54 degrees with a ground track that repeats every few days. This strongly indicates a likely remote sensing mission, perhaps by flight testing new payloads. While it likely has substantive maneuvering capability, to date, the X-37B has not approached or rendezvoused with any other space objects.

The secret deployment of multiple small satellites raises additional questions about the mission of the X-37B. It suggests that the X-37B may have a mission to serve as a covert satellite deployment platform. The secrecy surrounding both the X-37B and the deployment may indicate they are part of a covert intelligence program, but it may also indicate the testing of offensive technologies or capabilities. The failure to even catalog the deployed satellites, something that is done even for classified U.S. military and intelligence satellites, calls into question the trustworthiness of the public SSA data provided by the U.S. military.

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 Shuttle mission in 1990,[408] and matched the description

[403] Joseph Trevithick, "X-37B's Power Beaming Payload A Reminder Of Potential Orbital Microwave Anti-Satellite Weapons," TheDrive.com, May 19, 2020, https://www.thedrive.com/the-war-zone/33531/x-37bs-power-beaming-payload-a-reminder-of-potential-orbital-microwave-anti-satellite-weapons.

[404] "X-37B Orbital Test Vehicle," United States Air Force, September 1, 2018, https://www.af.mil/About-Us/FactSheets/Display/Article/104539/x-37b-orbital-test-vehicle/

[405] Joseph Trevithick, "Space Force Has A Unit Dedicated To Orbital Warfare That Now Operates The X-37B Spaceplane," TheDrive.com, Oct. 30, 2020, https://www.thedrive.com/the-war-zone/37361/space-force-has-a-unit-dedicated-to-orbital-warfare-that-now-operates-the-x-37b-spaceplane.

[406] Tyler Rogoway, "This Is Our First Look At The Secretive X-37B Spaceplane With Its Cargo Bay Doors Open," TheDrive.com, Sept. 15, 2020, https://www.thedrive.com/the-war-zone/36440/this-is-our-first-look-at-the-secretive-x-37b-spaceplane-with-its-cargo-bay-doors-open.

[407] Brian Weeden, "X-37B Orbital Test Vehicle Fact Sheet", Secure World Foundation, June 1, 2017, https://swfound.org/media/206982/swf_x-37b_otv_fact_sheet.pdf

[408] 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.

given in a 2004 NBC news article about a classified U.S. government satellite program that had run afoul of Congress.[409] 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 (USA 187, 2006-024A, 29240; USA 188, 2004-024B, 29241), with the official mission to identify, integrate, test, and evaluate small satellite technologies to support and enhance future U.S. space missions.[410] Observers speculated that the MiTEx satellites would be conducting RPO in GSO.[411] 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.[412] 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 Geosynchronous Space Situational Awareness Program, which may have the internal codename of Hornet. 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.[413] The official USAF fact sheet states that the GSSAP satellites are able to conduct RPO of "resident space objects of interest."[414] The first pair of GSSAP satellites (USA 253, 2014-043A; USA 254, 2014-043B) were launched on July 28, 2014, and the second pair (USA 270, 2016-052A; USA 271, 2016-052B) 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.[415] They are now operated by the 1st Space Operations Squadron of the USSF's Space Delta 9.[416]

On September 18, 2015, General John E. Hyten, then Commander of AFSPC, remarked at a public forum that the two GSSAP satellites had been "pressed into early service" to provide information to an un-named customer.[417] According to General Hyten, the two satellites provided what he deemed "eye-watering" pictures of one or more objects in GSO.

409 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/.

410 Justin Ray, "Experimental Military Microsatellites Reach Orbit," Spaceflight Now, June 22, 2006, https://www.space.com/2529-experimental-military-microsatellites-reach-orbit.html.

411 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.

412 Brian Weeden, "The Ongoing Saga of DSP Flight 23," TheSpaceReview.com, January 19, 2009, p.1, http://www.thespacereview.com/article/1290/1.

413 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.

414 "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/.

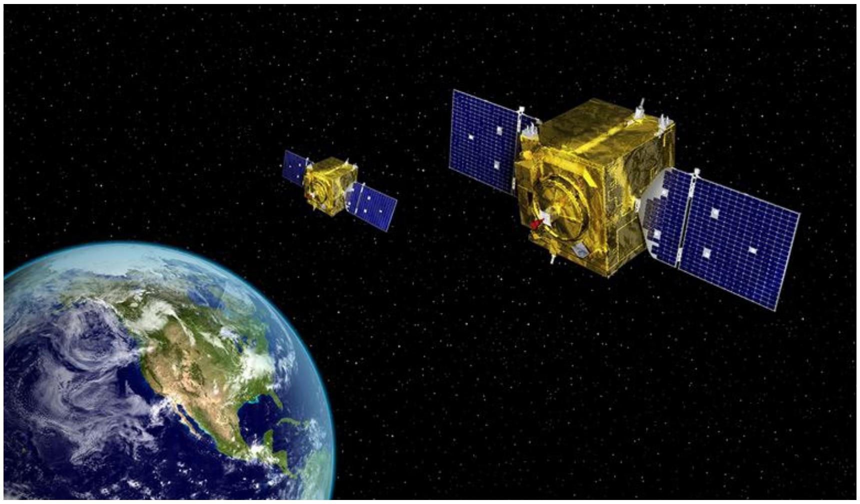
415 "GSSAP 1, 2, 3, 4, 5, 6," Gunter's Space Page, accessed March 22, 2018, http://space.skyrocket.de/doc_sdat/gssap-1.htm.

416 Joseph Trevithick, "Space Force Has A Unit Dedicated To Orbital Warfare That Now Operates The X-37B Spaceplane," TheDrive.com, Oct. 30, 2020, https://www.thedrive.com/the-war-zone/37361/space-force-has-a-unit-dedicated-to-orbital-warfare-that-now-operates-the-x-37b-spaceplane.

417 Mike Gruss, "Space Surveillance Sats Pressed Into Early Service," SpaceNews, September 18, 2015, http://spacenews.com/space-surveillance-sats-pressed-into-early-service/.

418 "Geosynchronous Space Situational Awareness Program," USAF Fact Sheets, March 22, 2017, https://www.afspc.af.mil/About-Us/Fact-Sheets/Display/Article/730802/geosynchronous-space-situational-awareness-program/.

FIGURE 15 - GSSAP SATELLITES



Artist's depiction. Image credit: U.S. Air Force.[418]

Although the U.S. military did not initially provide any public data on the locations or maneuvers of the GSSAP satellites, other sources of tracking data show they are very active in the GEO region. Data collected by the ISON space surveillance network, managed by the Russian Academy of Sciences, indicates that the GSSAP satellites have conducted hundreds of maneuvers since 2014 and have conducted close approaches or proximity operations of more than a dozen operational satellites in GEO, as summarized in Table 31 below. GSSAP has done close approaches of several U.S. military satellites and also several Russian or Chinese military satellites and commercial satellites built by China and operated by other countries. According to the Russian sources, some of these close approaches involved the GSSAP satellite making many small phasing maneuvers during a short period of time or conducting its close approach while both satellites passed through the Earth's shadow and could not be tracked by ground-based optical telescopes. These incidents made it very difficult to estimate the current and future position of the GSSAP satellite and the other object, creating difficulty in determining safe approaches and ascertaining the intent of the approach, which could lead to misperceptions and mistakes. Russian sources also claim GSSAP made more than fourteen one- and two-impulse maneuvers during their proximity operations of WGS 4 (2012-003A, 38070), a U.S. military communications satellite, which raised concerns about whether it was testing co-orbital technologies. The U.S. military began releasing public positional information for all four GSSAP satellites at the end of 2019, although some of the data is weeks or months old.

TABLE 07 - SATELLITES APPROACHED BY GSSAP[419]

DATE	SATELLITE APPROACHED	COUNTRY OF OWNERSHIP	APPROACH DISTANCE
Sept. 13, 2016	TJS-1	China	15 km
Jul. 13, 2017	Express AM-8	Russia	10 km
Sept. 14, 2017	Luch	Russia	10 km
Sept. 21, 2017	Paksat 1R	Pakistan	12 km
Sept. 29, 2017	Nigcomsat 1R	Nigeria	11 km
Oct. 5, 2017	Blagovest (Cosmos 2520)	Russia	14 km
Nov. 17, 2017	Raduga-1M 3	Russia	12 km
May 14, 2018	Raduga-1M 2	Russia	13 km

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.[420] 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 (USA 255, 2014-043C, 40101) stayed attached to the Delta 4 upper stage (2014-043D, 40102) 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.[421] Russian tracking sources indicate that during one close approach conducted on June 9, 2016, the Delta upper stage altered its orbit, suggesting it might not have been totally inert. The USAF originally did not disclose orbital information for either ANGELS or the Delta 4 upper stage but began to in February 2020. ANGELS was decommissioned in November 2017.[422]

On April 14, 2018, the United States conducted another military launch that placed multiple small satellites in GEO, including at least one that has conducted rendezvous and proximity operations.[423] The primary payload on the launch was the USAF's Continuous Broadcast Augmenting SATCOM (CBAS) military communications relay satellite, cataloged at USA 283 (2018-036A, 43339). The launch also included the Evolved Expendable Launch Vehicle (EELV) Secondary Payload Adapter (ESPA) Augmented Geosynchronous Laboratory Experiment satellite, known by the triple-nested acronym EAGLE but officially cataloged as USA 284 (2018-036B, 43340). The ESPA ring is commonly used for deploying small satellites as secondary payloads, and the EAGLE concept converts the ESPA ring from part of the launch vehicle into an independent maneuverable satellite, allowing for more flexible deployment of multiple small satellites.[424]

On this first launch, the EAGLE separated from the upper stage in the GEO region and subsequently deployed at least three small satellites. One of these small satellites, Mycroft (USA 287, 2018-036G, 43465),

419 Based on data provided by Vladimir Agapov, derived from tracking data collected by the ISON Space Surveillance Network.

420 Stephen Clark, "Air Force General Reveals New Space Surveillance Program," SpaceFlight Now, February 25, 2014, http://spaceflightnow.com/news/n1402/25gssap/.

421 "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.

422 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/.

423 Stephen Clark, "Multi-satellite payload hoisted into high altitude orbit by Atlas 5 rocket," Spaceflightnow.com, April 15, 2018, https://spaceflightnow.com/2018/04/15/multi-satellite-stack-hoisted-into-high-altitude-orbit-by-atlas-5-rocket/.

424 Air Force Research Laboratory, "ESPA Augmented Geosynchronous Laboratory Experiment (EAGLE)", ABW Public Affairs fact sheet, April 2018, https://www.kirtland.af.mil/Portals/52/documents/EAGLE-factsheet.pdf.

separated from EAGLE in early May 2018 and conducted a series of close approaches to EAGLE. The name Mycroft refers to the older and smarter brother of the fictional detective Sherlock Holmes, and the USAF describes it as demonstrating "improved space situational awareness for space vehicles."[425] The U.S. military has not provided any information on the other two payloads. In January 2020, the U.S. military began providing public orbital information for CBAS, the Centaur upper stage, and the other two unnamed payloads but not EAGLE or Mycroft.[426]

In October 2019, the USAF announced that Mycroft was being sent to inspect another U.S. satellite in the GEO region, S5 (2019-009D, 44065).[427] S5 was an experimental satellite launched into GEO on February 22, 2019, to test out new space situational awareness concepts, but stopped communicating with ground controllers in March 2019.[428] The USAF stated that Mycroft would conduct a series of RPO maneuvers with S5 over a period of weeks to try and determine the

TABLE 08 - RECENT U.S. RPO ACTIVITIES

DATE(S)	SYSTEM(S)	ORBITAL PARAMETERS	NOTES
Jan. 2003	XSS-10, Delta R/B	800 x 800 km; 39.6°	XSS-10 did a series of maneuvers to bring it within 50 meters of the Delta upper stage that placed it in orbit
Apr. 2005 – Oct. 2006	XSS-11, multiple objects	LEO	XSS-11 did a series of maneuvers to bring it close to the Minotaur upper stage that placed it in orbit. it then performed additional close approaches to other U.S. space objects in nearby LEO orbits over the next 12-18 months
Mar. – Jul. 2007	ASTRO, NEXTSat	LEO	ASTRO and NEXTSat were launched together and performed a series of separations, close approaches, and dockings with each other
Jul. 2014 – present	GSSAP, multiple objects	GEO	Two pairs of GSSAP satellites have been performing RPO with various other objects in the GEO region
Jul. 2014 – Nov. 2017	ANGELS, Delta 4 R/B	GSO	ANGELS separated from the Delta 4 upper stage that placed the first GSSAP pair into orbit and then performed a series of RPO in the GSO disposal region
May 2018	Mycroft, EAGLE	GEO	EAGLE separated from the Delta V upper stage, and Mycroft subsequently separated from EAGLE. Mycroft conducted RPO of EAGLE in the GEO region
Oct. 2019	Mycroft, S5	GEO	Mycroft maneuvered to rendezvous with S5 after the latter ceased communications

status of the latter's solar arrays and antennas. Amateur observers noted that Mycroft was communicating using a largely "suppressed" carrier signal, making it more difficult to detect.[429]

POTENTIAL MILITARY UTILITY

The most likely military utility of the capabilities demonstrated by the DART, XSS-10, XSS-11, Orbital Express, Prowler, MiTEx, GSSAP, ANGELS, and Mycroft 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

[425] 88th Air Base Wing Public Affairs, "Successful launch for AFRL Eagle spacecraft experiment on AFSPC-11 mission," Schriever Air Force Base, April 18, 2018, https://www.schriever.af.mil/News/Article-Display/Article/1496633/successful-launch-for-afrl-eagle-spacecraft-experiment-on-afspc-11-mission/.

[426] Data compiled from the public satellite catalog maintained by the U.S. military at https://space-track.org

[427] Rachel Cohen, "AFRL Dispatching Satellite to Examine Unresponsive Smallsat," Air Force Magazine, October 18, 2019, https://www.airforcemag.com/AFRL-Dispatching-Satellite-to-Examine-Unresponsive-Smallsat/

[428] Ibid.

[429] Scott Tilley, tweet posted December 21, 2019, https://twitter.com/coastal8049/status/1208475681790627841?s=20

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 (See Chinese Co-Orbital ASAT; section 1.1) and the Russian Cosmos 2499, Luch, and Cosmos 2521 satellites (See Russian Co-Orbital ASAT; section 2.1). 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

During the Cold War, the U.S. military had multiple efforts to develop DA-ASAT capabilities. Some of those efforts remained on the drawing board and several were tested in space, but none reached operational status.

Bold Orion and High Virgo — U.S. DA-ASAT capabilities began as final tests of already existing anti-ballistic missile (ABM) weapons. Because midcourse missile defense systems are intended to destroy nuclear warheads that travel through outer space at speeds and altitudes comparable to those of satellites, such midcourse ABM systems also have inherent ASAT capabilities. In the late 1950s and early 60s, the US tested many air-launched ballistic missiles (ALBM) as part of efforts to defend against Soviet ICBMs. At the end of the testing period, the final ALBM tests of the Bold Orion and High Virgo were used to validate the feasibility of destroying a satellite with ballistic missile technology.[430] These tests led to development of the first DA-ASAT program built from the Nike Zeus anti-ballistic missile.

HiHo — During the 1960s, the U.S. Navy was also researching possible ASAT capabilities. Early efforts focused on matching a Navy Sparrow anti-aircraft missile with a Polaris Submarine-Launched Ballistic Missile (SLBM) but these efforts did not proceed beyond ground experiments.

[430] Andreas Parsch, "WS-199," Directory of U.S. Military Rockets and Missiles, Updated November 1, 2005, http://www.designation-systems.net/dusrm/app4/ws-199.html.

However, in 1962 the Navy began work on Project HiHo, which involved a Caleb rocket fired from a Phantom 4D fighter bomber aircraft.[431] Although the primary focus was on developing an air-launched SLV, a secondary objective was to develop ASAT capabilities. Two test launches in space were conducted in 1962; the first one failed but the second reached an apogee of 1,600 kilometers (1,000 miles). In the end, the Navy decided not to pursue an operational version.

Nike Zeus — The Nike Zeus ASAT Program was developed out of anti-ballistic missile testing of the U.S. Army's Nike Zeus system and later came to be known as Program 505. Beginning in 1957, the U.S. Army argued that its Nike-Zeus ABM system could have an ASAT capability added to it to help defend against ICBMs and space threats.[432] In 1962, the proposal was approved and Project Mudflap, later named Nike Zeus, began development. Nike Zeus consisted of a modified three-stage solid fuel Nike rocket tipped with a one-megaton nuclear warhead. It was believed that detonating the warhead in close proximity to a target satellite would disable it either through the resultant fireball or EMP. In May 1963, a modified Zeus B missile successfully intercepted an Agena D rocket stage in orbit, marking a key success of the program's new capability and extension to Kwajalein Atoll.[433] Testing continued over the course of the early 1960s but eventually gave way to Program 437 which demonstrated greater performance and would extend through the remainder of the decade.

Program 437 — Similar to Nike Zeus/Program 505, Program 437 was developed from ABM technology but replaced the Nike Zeus with a Thor missile allowing for longer range capabilities.[434] Program 437 could target satellites orbiting as high as 1,300 kilometers and used a 1.4-megaton W49 nuclear warhead with a likely kill radius of eight kilometers.[435] The missiles and warheads were stored at Vandenberg AFB in California, while the Thors were operated out of the Johnson Atoll, so they required a two-week notification to get the missiles and warheads to their launch vehicle.[436] On August 6, 1963, President Kennedy directed that Program 437 be given the highest national priority category for further research and development.[437] It was tested multiple times against rocket bodies and other space debris to assure the missile could pass within the kill radius without destroying the object and creating unnecessary debris. It remained operational on Johnston Atoll until the early 1970s and was formally terminated in 1975.[438]

431 John Pike, "HiHo / Hi-Hoe / NOTS-EV-2 Caleb," GlobalSecurity.org, accessed February 24, 2021, https://www.globalsecurity.org/space/systems/hiho.htm.

432 Paul Stares, The Militarization of Space: U.S. Policy, 1945-1984, Cornell University Press, August 1, 1985, pg 117.

433 Brian Weeden, "Through a Glass, Darkly Chinese, American, and Russian Anti-satellite Testing in Space," TheSpaceReview, March 17, 2014, https://swfound.org/media/167224/through_a_glass_darkly_march2014.pdf.

434 Curtis Peebles, "High Frontier: The U.S. Air Force and the Military Space Program," Air Force History and Museums Program, 1997, https://www.google.com/books/edition/_/cMgdYypcPc8C?hl=en&gbpv=1&pg=PP1

435 Paul Stares, "The Militarization of Space: U.S. Policy, 1945-1984," Cornell University Press, August 1, 1985, https://www.google.com/books/edition/The_Militarization_of_Space/2asgAAAAMAAJ?hl=en&gbpv=0.

436 Mark Wade, "Program 437," Astronautix.com, http://www.astronautix.com/pprogram437.html, accessed Feb. 19, 2021.

437 McGeorge Bundy, "Assignment of the Highest National Priority to Program 437," The White House, National Security Action Memorandum No. 258, August 6, 1963, https://fas.org/irp/offdocs/nsam-jfk/nsam258.jpg.

438 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.

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.[439] 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.[440] Five flight tests occurred,[441] the most famous of which was an intercept test on September 13, 1985, in which the Solwind P78-1 satellite (1979-017A, 11278) was destroyed at an altitude of 555 km, marking the only time that a U.S. missile destroyed a satellite prior to 2008.[442]

The ASM-135 had an estimated operational range of 648 km, flight ceiling of 563 km, and speed of over 24,000 km/h.[443] 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.[444]

The USAF had planned to deploy an operational force of 112 ASM-135 missiles, to be deployed aboard 20 modified F-15s.[445] 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.

439 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.

440 Ibid.

441 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.

442 "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/.

443 Parsch, "Vought ASM-135 ASAT."

444 "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.

445 Parsch, "Vought ASM-135 ASAT."

TABLE 09 - HISTORY OF U.S. DA-ASAT TESTING

DATE	ASAT SYSTEM	SITE	TARGET	APOGEE	NOTES
Sept. 22, 1959	High Virgo	Unknown	None	12 km	Unknown results due to loss of telemetry
Oct. 13, 1959	Bold Orion	Unknown	Explorer VI	200 km	Success (passed within kill radius)
April 1962	HiHo	Unknown	None	Unknown	Failure
July 1962	HiHo	Unknown	None	1,600 km	Successful rocket test
Dec. 17, 1962	Nike Zeus	WSMR	None	160 km	Success (reached designated point in space)
Feb. 15, 1963	Nike Zeus	Kwajalein	None	241 km	Successful intercept of designated point in space
Mar. 31, 1963	Nike Zeus	Kwajalein	None	-	Unsuccessful attempt to intercept simulated satellite target
Apr. 19, 1963	Nike Zeus	Kwajalein	None	-	Unsuccessful attempt to intercept simulated satellite target
May 24, 1963	Nike Zeus	Kwajalein	Agena D	Unknown	Successful close intercept
Jan. 4, 1964	Nike Zeus	Kwajalein	None	146 km	Successful intercept of a simulated satellite target
Feb. 14, 1964	Program 437	Johnston Island	Transit 2A Rocket Body	1000 km	Success (passed within kill radius)
Mar. 1, 1964	Program 437	Johnston Island	Unknown	674 km	Success (primary missile scrubbed, backup missile passed within kill radius)
Apr. 21, 1964	Program 437	Johnston Island	Unknown	778 km	Success (passed within kill radius)
May 28, 1964	Program 437	Johnston Island	Unknown	932 km	Failed (missed intercept point)
Nov. 16, 1964	Program 437	Johnston Island	Unknown	1,148 km	Successful Combat Test Launch (passed within kill radius)
Nov. 16, 1964	Program 437	Johnston Island	Unknown	1,148 km	Successful Combat Test Launch (passed within kill radius)
Apr. 1965	Nike Zeus	Kwajalein	None	Unknown	-
Apr. 5, 1965	Program 437	Johnston Island	Transit 2A Rocket Body	826 km	Successful Combat Test Launch (passed within kill radius)
June-July 1965	Nike Zeus	Kwajalein	None	Unknown	Four test intercepts, of which three were successful
Jan. 13, 1966	Nike Zeus	Kwajalein	None	Unknown	Successful intercept with simulated target
Mar. 31, 1967	Program 437	Johnston Island	Unknown piece of space debris	484 km	Successful Combat Evaluation Launch (passed within kill radius)
May 15, 1968	Program 437	Johnston Island	Unknown	823 km	Successful Combat Evaluation Launch (passed within kill radius)
Nov. 21, 1968	Program 437	Johnston Island	Unknown	1,158 km	Successful Combat Evaluation Launch (passed within kill radius)
Mar. 28, 1970	Program 437	Johnston Island	unknown satellite	1,074 km	Success (passed within kill radius)
Jan. 21, 1984	ASM-135	aircraft	None	1,000 km	ASM-135 missile fired from F-15 fighter, successful missile test
Nov. 13, 1984	ASM-135	aircraft	Star	1,000 km	Failed test
Sept. 13, 1985	ASM-135	aircraft	Solwind	555 km	Successful test, created 285 pieces of trackable orbital debris
Aug. 22, 1986	ASM-135	aircraft	Star	1,000 km	Successful test in tracking
Sept. 29, 1986	ASM-135	aircraft	Star	1,000 km	Successful test in tracking
Feb. 20, 2008	SM-3	USS Lake Erie	USA 193	2,700 km	Successful test

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.[446] 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,[447] with plans underway to deploy an additional 20 interceptors.[448] The planned burnout speed of the GBIs is reported to be 7 to 8 km/s.[449] 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.

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.[450] However, the SM-3 Block IIA interceptors, currently under joint development with Japan,

[446] "Navy Missile Hits Dying Spy Satellite, Says Pentagon," CNN, February 21, 2008, http://www.cnn.com/2008/TECH/space/02/20/satellite.shootdown/.

[447] "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/.

[448] Jen Judson, "Where are the laser-armed drones? Missile Defense Review wish list missing from MDA's budget," Defense News, March 12, 2019, https://www.defensenews.com/smr/federal-budget/2019/03/13/missile-defense-review-ambitions-not-reflected-in-mdas-94b-fy20-budget/.

[449] 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.

[450] 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.

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 3-4. 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 10 - MAXMIMUM ALTITUDE REACHABLE BY SM-3 VARIANTS[451]

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 intended to be deployed at land-based "Aegis Ashore" sites. The initial land-based Aegis Ashore site in Romania is in operation.[452] A future site is being developed in Poland; at one point, Japan was planning on joining the Aegis Ashore program, but cancelled construction in June 2020.[453] The number of ballistic missile defense (BMD)-capable Aegis ships is expected to go from 48 (end of FY2021) to 65 (end of FY2025)[454] and any of their hundreds of interceptors could be ASAT-capable.

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.[455] 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.[456]

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

451 Ibid.

452 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.

453 Michael Unbehauen & Christian Decker, "Japan Cancels Aegis Ashore: Reasons, Consequences, and International Implications," Journal of Indo-Pacific Affairs, Air University Press, September 25, 2020, https://www.airuniversity.af.edu/JIPA/Display/Article/2361398/japan-cancels-aegis-ashore-reasons-consequences-and-international-implications/.

454 Ronald O'Rourke, Navy Aegis Ballistic Missile Defense (BMD) Program: Background and Issues for Congress, Congressional Research Service report RL33745, updated December 23, 2020, https://fas.org/sgp/crs/weapons/RL33745.pdf, p.5.

455 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.

456 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.h

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.

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. It is working on Meadowlands, an updated version of the CCS system, which is intended to be used in an offensive capacity against satellite communications.

The United States has regularly exercised the capability to jam Global Navigation Satellite System (GNSS) receivers (GPS, GLONASS, Beidou) within a local or regional 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.[457]

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 (February 2020), the description has evolved somewhat offering more insight on the role of the CCS. [458]

[457] "RDT&E Budget Item Justification Sheet (R-2 Exhibit), PE Number: 0604421F, PE Title: Counterspace Systems," Air Force, February 2003: p. 883, https://www.saffm.hq.af.mil/Portals/84/documents/FY04/AFD-070223-060.pdf?ver=2016-08-22-101828-843

[458] RDT&E Budget Item Justification: FY 2021 Space Force, Program Element: PE 1206421F / Counterspace Systems, project 65A001 / Counter Satellite Communications System, February 2020: p. 111, https://www.saffm.hq.af.mil/Portals/84/documents/FY21/RDTE_/FY21%20Space%20Force%20Research%20Development%20Test%20and%20Evaluation.pdf?ver=2020-02-11-083608-887

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 the 4th Space Control Squadron 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.[459]

The first two CCS units were reportedly delivered in 2004.[460] 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.[461] In 2014, Harris again was awarded a contract to upgrade the Block 10.1 systems to the Block 10.2 configuration and deliver a total of 16 Block 10.2 systems to the 4th Space Control Squadron as well as Air National Guard units.[462] In March 2020, CCS Block 10.2 was announced to have reached initial operating capability and was deemed to be the USSF's first offensive weapon.[463]

The total number of current U.S. CCS units is not publicly known, but there are at least 13 units. In March 2017, Harris was awarded a contract to provide Block 10.2 upgrades for 13 existing antennas across the CCS.[464]

In April 2020, the USAF announced Meadowlands as a further block upgrade to CCS 10.2. It is intended to be lighter than the CCS system, jam a broader spectrum of frequencies, and use open architecture software to allow for easier updates.[465] It is being built by L3Harris with the goal of delivering four systems by April 2023; the USSF intends to launch a competition for 28 more units.[466]

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. From 2004 to 2017, approximately $222 million was spent on the CCS program. The projected spending for FY21-FY25 totals an additional $174 million.[467]

[459] "76th Space Control Squadron Fact Sheet," Peterson AFB web site, August 16, 2012, https://www.peterson.spaceforce.mil/About/Fact-Sheets/Display/Article/326218/76th-space-control-squadron/

[460] Jeffrey Lewis, "Counter Satellite Communications System Deployed," ArmsControlWonk.com, October 2, 2004, https://www.armscontrolwonk.com/archive/200025/counter-satellite-communications-system-deployed/.

[461] George I. Seffers, "Harris to Upgrade Counter Communication Systems," Signal, November 13, 2002, https://www.afcea.org/content/harris-upgrade-counter-communication-systems.

[462] Sandra Erwin, "U.S. Space Force Gets Upgraded Satellite Communications Jammers for 'Offensive' Operations," SpaceNews, February 4, 2020, https://spacenews.com/u-s-space-force-gets-upgraded-satellite-communications-jammers-for-offensive-operations/

[463] "Counter Communications System Block 10.2 achieves IOC, ready for the warfighter," Space and Missile Systems Public Affairs, March 13, 2020, https://www.spaceforce.mil/News/Article/2113447/counter-communications-system-block-102-achieves-ioc-ready-for-the-warfighter/.

[464] "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.

[465] Anthony Capaccio, "U.S. Builds Ground-Based Arsenal to Jam Russia, China Satellites," Bloomberg Quint, April 17, 2020, https://www.bloombergquint.com/politics/u-s-space-force-is-arming-to-jam-russian-and-chinese-satellites.

[466] Frank Wolfe, "Space Force Developing Non-Kinetic Counterspace Systems," Defense Daily, Nov. 9, 2020, https://www.defensedaily.com/space-force-developing-non-kinetic-counterspace-systems/space/.

[467] RDT&E Budget Item Justification: FY 2021 Space Force, Program Element: PE 1206421F / Counterspace Systems, project 65A001 / Counter Satellite Communications System, February 2020: p. 111, https://www.saffm.hq.af.mil/Portals/84/documents/FY21/RDTE_/FY21%20Space%20Force%20Research%20Development%20Test%20and%20Evaluation.pdf?ver=2020-02-11-083608-887

There is no public information on theater deployments, if any, by the CCS. A USSF press release in March 2020 noted that CCS was used by USAF active duty units and Air National Guard units in California, Colorado, and Florida.[468] 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.[469]

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."[470]

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 the first GPS Block IIR-M satellite (NAVSTAR 57, 2005-038A, 28874) launched on September 26, 2005 will be able to broadcast M-code. There are currently 21 M-code capable GPS satellites, including the first of the new GPS Block IIIA satellites launched on December 23, 2018.[471] Deployment of the ground control system (known as OCX) and new end user receivers

[468] Space and Missile Systems Center Public Affairs, "Counter Communications System Block 10.2 achieves IOC," United States Space Force, March 13, 2020, https://www.spaceforce.mil/News/Article/2113447/counter-communicationssystem-block-102-achieves-ioc-ready-for-the-warfighter/.

[469] 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.

[470] "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/.

[471] Doug Messier, "Final Steps Underway To Operationalize Ultra-Secure, Jam-Resistant GPS M-Code Signal," Parabolic Arc, March 30, 2020, http://www.parabolicarc.com/2020/03/30/final-steps-underway-to-operationalize-ultra-secure-jam-resistant-gps-m-code-signal/.

to fully implement and utilize M-code have run into significant delays and challenges.[472] Six USSF sites are receiving new software-defined receivers that will allow for M-code to be enabled to meet the goal of protecting from spoofing and jamming. The effectiveness of these measures, against a sophisticated adversary, is not known,[473] and it will take a significant period of time to roll out upgrades or new receivers to the 700+ deployed weapon systems that utilize GPS.[474]

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 accomplished is by using downlink jamming to interfere with or spoof GNSS signals in a specific geographic area.[475] The U.S. military is known to exercise the ability to jam GNSS or operate while adversary jamming is taking place. In January 2018, the USAF announced it would be jamming the civil GPS signals across the Nevada Test and Training Range as part of its annual Red Flag exercise.[476] In August 2018 and February 2019, a U.S. Navy Carrier Strike Group also exercised wide-scale jamming of GPS across the southeastern coast of the United States.[477] Additional wide-scale jamming was exercised in the southeastern coast of the United States on August 30, 2019, and September 5, 2019,[478] and January 16-24, 2020.[479]

POTENTIAL MILITARY UTILITY

The Counter Communications System is likely very effective in denying potential adversaries of geostationary satellite communications capabilities, and the new upgrades even more so. 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 on 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.

However, conducting operationally-useful, dependable, and reliable jamming of highly-used military space capabilities, such as GNSS, is more difficult than most commentators suggest. Military GNSS signals are much more resilient to jamming than civil GNSS signals, and a wide variety of tactics, techniques, and procedures exist to mitigate attacks.[480] It is much more likely that an EW counterspace weapon would degrade military space capabilities rather than completely deny them.

472 "Global Positioning System: Updated Schedule Assessment Could Help Decision Makers Address Likely Delays Related to New Ground Control System," Government Accountability Office, GAO-19-250, May 21, 2019, https://www.gao.gov/assets/700/699234.pdf.

473 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/.

474 Michael Jones, "New Military Code About to Board 700+ Platforms," GPS World, April 9, 2019, https://www.gpsworld.com/new-military-code-about-to-board-700-platforms/

475 Daniel Cebul, "DoD jams GPS in western states for joint exercise", C4ISR Net, January 26, 2018, https://www.c4isrnet.com/specialreports/pnt/2018/01/26/dod-jams-gps-in-western-states-for-joint-exercise/.

476 Tyler Rogoway, "USAF is jamming GPS in the Western U.S. for largest ever Red Flag air war exercise," The Drive, January 25, 2018, http://thedrive.com/the-war-zone/17987/usaf-is-jamming-gps-in-the-western-u-s-for-largest-ever-red-flag-air-war-exercise.

477 David Cenciotti, "Basically, Carrier Strike Group 4 is jamming GPS across the U.S. Southeast coast," The Aviationist, February 8, 2019, https://theaviationist.com/2019/02/08/basically-carrier-strike-group-4-is-jamming-gps-across-u-s-southeast-coast/.

478 Tracy Cozzens, "U.S. Navy to Conduct GPS Interference Tests Off Savannah," GPS World, August 30, 2019, https://www.gpsworld.com/u-s-navy-to-conduct-gps-interference-tests-off-savannah/

479 Tom Demmerly, "U.S. Navy Now Jamming GPS Over Six States and 125,000 Square Miles," The Aviationist, January 23, 2020, https://theaviationist.com/2020/01/23/u-s-navy-now-jamming-gps-over-six-states-and-125000-square-miles/

480 Brandon Davenport and Rich Ganske, "Recalculating Route: A Realistic Risk Assessment for GPS," War on the Rocks, March 11, 2019, https://warontherocks.com/2019/03/recalculating-route-a-realistic-risk-assessment-for-gps/.

3.4 – U.S. DIRECTED ENERGY WEAPONS

ASSESSMENT

Over the past several decades, the United States has conducted significant research and development on the use of ground-based high energy lasers for counterspace and other purposes. We assess that there are no technological roadblocks to the U.S. operationalizing them for counterspace applications. With its SLR sites and defense research facilities, the United States possesses low power laser systems with the capability to dazzle, and possibly blind, EO imaging satellites. However, there is no indication that these potential high or low power capabilities have been operationalized.

There is no public evidence that the United States has a space-based DEW capability. However, the Missile Defense Agency (MDA) is planning to conduct research into the feasibility of space-based DEW for defending against ballistic missiles. If developed, these systems may have a capability against other orbiting satellites and, depending on their target acquisition and tracking capabilities, may be considered de facto anti-satellite systems.

SPECIFICS

Over the past several decades, the United States has sufficiently developed the technologies required to construct and deploy a ground-based counterspace laser weapon that would be capable of damaging most types of LEO satellites. However, there is no public indication that the United States has transitioned from a research phase to an operational capability.

Most of the historical activities and research was connected to the Strategic Defense Initiative (SDI) in the 1980s and focused on high-power lasers that could be used to intercept ballistic missiles or nuclear warheads but could also be used against satellites. The most publicized U.S. counterspace laser research project involves the Mid-Infrared Advanced Chemical Laser (MIRACL) Program. MIRACL is a chemical laser (deuterium fluoride) capable of emitting a multi-megawatt beam in the infrared spectrum. The project was initially funded by the Strategic Defense Initiative Office (SDIO), beginning in 1985, for the purpose of conducting research to defend against ballistic missiles.[481] MIRACL was fired against an orbiting satellite in October 1997. The target was the MSTI-3 satellite, a USAF experimental satellite that had been launched in May 1996 and had completed its mission. MSTI-3 carried IR sensors and was an ideal target for an IR laser. Detailed results of the test were not made public. Official statements by the Pentagon indicated that the test was defensive in nature with the purpose of gathering data to “improve computer models used for planning the protection of U.S. satellites” and the Pentagon further stated that ''there's absolutely no intention to use the laser for offensive purposes.” [482]

[481] White Sands Missile Range, “High Energy Laser Systems Test Facility,” updated October 26, 2018, https://www.wsmr.army.mil/testcenter/testing/landf/Pages/HighEnergyLaserSystemsTestFacility.aspx

[482] William Broad, “U.S. to Fire Laser Weapon at a Satellite,” New York Times, October 3, 1997, https://www.nytimes.com/1997/10/03/us/us-to-fire-laser-weapon-at-a-satellite.html.

Regardless of assurances as to the intent of the test, the capability of MIRACL to damage satellites in orbit appeared to have been demonstrated. MIRACL continued to be used for research on other high-power laser applications, such as defense against rockets and missiles, until at least the mid-2000's.[483] The MIRACL laser appears to still be actively used in research projects and remains a key component of the High Energy Laser Systems Test Facility at the U.S. Army's White Sands Missile range.[484]

Another notable example was the Low-Power Atmospheric Compensation Experiment (LACE) satellite, launched in 1990, which was a Naval Research Laboratory project sponsored by SDIO. The satellite carried three separate sensor arrays capable of characterizing ground-based laser beams of various types and wavelengths. The sensors determined the power received from ground-based lasers and was used to determine the effectiveness of various methods of compensating for atmospheric distortion, an important consideration for ground-based laser ASAT systems.

A third example was the Airborne Laser Testbed (ABL), a USAF/Missile Defense Agency (MDA) project, begun in 1996, to test the feasibility of intercepting ballistic missiles in their boost phase using a high-power laser installed in a Boeing 747 aircraft. The aircraft carried a megawatt class chemical oxygen iodine laser (COIL) along with two lower power lasers for target identification and tracking. During its lifetime, the project demonstrated capabilities by conducting several intercept tests of aerodynamic and ballistic targets. The project came under budget pressure and was cancelled in 2011. This project did not have a counterspace objective and did not directly develop capabilities to target satellites, although some technologies may be able to contribute to counterspace applications.

There is no indication that the United States has developed the technology required for the building blocks of a space-based laser ASAT capability, nor has it been a goal since the early days of SDI in the 1980s. There is not publicly-available evidence to suggest that the United States currently has a space-based laser counterspace capabilities and there are likely significant technological obstacles to fielding such a capability. However, there was an effort under SDI to develop space-based neutral particle beams. In 1989, the BEAM Experiment Aboard Rocket used a linear accelerator mounted inside an upper stage to test the propagation of a neutral particle beam in the outer space environment on a suborbital vehicle.[485] The experiment was deemed a success in that it successfully generated a neutron particle beam, albeit at extremely low power and for only a short period of time. To date there appears to have been little further development of the technology.

The United States has also conducted significant historical research and development on HPM for broad military applications and terrestrial use. One such application is the Active Denial System; a prototype non-lethal system to be used for at short ranges for stopping, deterring and turning

[483] Defense Advanced Research Projects Agency (DARPA), "MIRACL," accessed February 23, 2019, https://www.darpa.mil/about-us/timeline/miracl.

[484] White Sands Missile Range, "High Energy Laser Systems Test Facility," updated October 26, 2018, https://www.wsmr.army.mil/testcenter/testing/landf/Pages/HighEnergyLaserSystemsTestFacility.aspx

[485] P. G. O'Shea, T. A. Butler, M. T. Lynch, K. F. McKenna, M. B. Pongratz, T. J. Zaugg, "A Linear Accelerator In Space: The Beam Experiment Aboard Rocket," Proceedings of the Linear Accelerator Conference 1990, Albuquerque, New Mexico, USA, https://accelconf.web.cern.ch/accelconf/l90/papers/th454.pdf.

back suspicious individuals with minimal risk of injury.[486] Although, in theory, an HPM weapon in space could damage a satellite if it was sufficiently close, there is no indication of any space-based capability or intent to pursue such by the United States. Current U.S.

DEW DEVELOPMENTS AND CAPABILITIES

The U.S. military is investing significant research and development funds in various DEW weapons applications. High power laser prototypes are being developed for tactical use, such as defense against missiles, rockets, artillery and UAVs.[487, 488] While none of these prototypes can be used for a counterspace role, they are furthering the development of component technologies that may be applicable to counterspace applications.

The United States currently operates several SLR sites, most of which are operated by either NASA or universities. The lone DoD site, the NRL Optical Test Facility at Stafford, VA, would be the likeliest of the ILRS sites to conduct laser dazzling tests or operations. However, there is no indication that this has occurred. Although it is theoretically possible to use SLR facilities to conduct laser dazzling, it is assessed that these sites are not a counterspace threat due to most of them being civilian. Furthermore, laser dazzling would only be useful if the SLR site was geographically located near a sensitive facility so that it could dazzle adversary imaging satellites as they came overhead from imaging that sensitive facility.

More recently, there has been a renewed discussion in the United States of some of the SDI missile defense initiatives that could also have counterspace applications. The SDIO transitioned into the Ballistic Missile Defense Organization (BMDO) in 1994 which was then renamed MDA in 2002. The 2019 Missile Defense Review conducted by the Pentagon under the Trump Administration proposed revisiting the original SDI concept of placing interceptor systems in orbit. Citing major improvements in technologies applicable to space-basing and directed energy, the review directs the DOD to study space-based defenses, which may include on-orbit demonstrations of concepts and technology.[489] Although the funding that will be devoted specifically to the space-based intercept options has not yet been revealed, at least $15 million is reported to be allocated to the exploration of space-based lasers for boost phase intercept.[490] The MDA's budget request for 2020 includes $304 million for technology maturation, some of which will be devoted to neutral particle beam and laser technologies, including testing a neutral particle beam weapon in orbit by 2023, but the plan has yet to receive Congressional approval and funding.[491]

It is not clear if the proposed studies into space-based defenses will include both boost and midcourse phases of ballistic missile flight. Although there have been statements suggesting that the studies into laser space-based defense concepts will address boost phase intercept,[492] that limitation is not specified in the 2019 Missile Defense Review nor in the budget request information that has been made public.

486 Active Denial Technology Fact Sheet, U.S. Department of Defense Non-Lethal Weapons Program, May 11, 2016. https://jnlwp.defense.gov/Portals/50/Documents/Press_Room/Fact_Sheets/ADT_Fact_Sheet_May_2016.pdf.

487 U.S. Army Weapons-Related Directed Energy (DE) Programs: Background and Potential Issues for Congress, Congressional Research Service, Updated February 12, 2018. https://crsreports.congress.gov/product/pdf/R/R45098.

488 Navy Lasers, Railgun, and Gun-Launched Guided Projectile: Background and Issues for Congress, Congressional Research Service, Updated October 23, 2018. https://crsreports.congress.gov/product/pdf/R/R44175.

489 2019 Missile Defense Review, Office of the Secretary of Defense, January 17, 2019, https://www.defense.gov/Portals/1/Interactive/2018/11-2019-Missile-Defense-Review/The%202019%20MDR_Executive%20Summary.pdf

490 Patrick Tucker, "Pentagon Wants to Test A Space-Based Weapon in 2023," Defense One, March 14, 2019. https://www.defenseone.com/technology/2019/03/pentagon-wants-test-space-based-weapon-2023/155581/.

491 Transcript of Department of Defense Press Briefing on the President's Fiscal Year 2020 Defense Budget for the Missile Defense Agency, U.S. Department of Defense, March 12, 2019. https://dod.defense.gov/NewsTranscripts/Transcript-View/Article/1784150/department-of-defense-press-briefing-on-the-presidents-fiscal-year-2020-defense/.

492 Patrick Tucker, "Pentagon Wants to Test A Space-Based Weapon in 2023," Defense One, March 14, 2019, https://www.defenseone.com/technology/2019/03/pentagon-wants-test-space-based-weapon-2023/155581/.

The difference between boost phase and midcourse phase concepts are significant for ASAT capability. The tracking and pointing requirement for a boost phase intercept are different from that which would be required of an ASAT. However, the requirements for a midcourse phase intercept would be very similar, leading to the assessment that a midcourse intercept capability equates to an ASAT capability. Regardless of the technical details of the concepts being studied, potential adversaries are likely to interpret this initiative as research and development into both ballistic missile defense and ASAT capabilities.

This MDA initiative to study concepts marks only an initial step towards a possible future space-based BMD and ASAT capability. Numerous technological and budgetary obstacles remain and it will likely be several years before substantial progress towards an actual capability could possibly be achieved, with no certainty of eventual success. The MDA is also planning to conduct research into the feasibility of placing a high-power laser on airborne platforms to intercept ballistic missiles in the boost phase. Even if successful, this approach will likely not result in a counterspace capability since the target acquisition and tracking requirements are substantially different.

MILITARY UTILITY

DEWs, primarily lasers, offer significant potential for military counterspace applications. They offer the possibility of interfering with or disabling a satellite without generating significant debris. The technologies required for ground-based lasers systems are well developed. Ground-based systems can dazzle or blind EO satellites, or even inflict thermal damage on most LEO satellites.

In contrast, the technical and financial challenges to space-based DEW for counterspace remain substantial. These include mass of the weapon, consumables and disturbance torques (chemical lasers), electrical power generation (solid state and fiber lasers, particle beams), target acquisition and tracking, and the potential required large size of constellation. The acquisition and tracking challenges are greatly simplified in a co-orbital GEO or LEO scenario.

However, both ground- and space-based DEW counterspace capabilities do have significant drawbacks in assessing their effectiveness. 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 a non-destructive DEW attack actually worked.

3.5 – U.S. SPACE SITUATIONAL AWARENESS CAPABILITIES

ASSESSMENT

The United States currently possesses the most advanced SSA capabilities in the world, particularly for military applications. U.S. SSA capabilities date to the beginning of the Cold War and leverage significant infrastructure developed for missile warning and missile defense. The core of its SSA capabilities is a robust, geographically dispersed network of ground-based radars and telescopes and space-based telescopes. The United States is investing heavily in upgrading its SSA capabilities by deploying new radars and telescopes in the Southern Hemisphere, upgrading existing sensors, and signing SSA data sharing agreements with other countries and satellite operators. The United States still faces challenges in modernizing the software and computer systems used to conduct SSA analysis and is increasingly looking to leverage commercial capabilities.

SPECIFICS

Like Russia, the United States developed its original SSA capabilities as part of the Cold War space and nuclear rivalry. The U.S. Space Surveillance Network (SSN) consists of multiple phased array radars that are primarily used for missile warning along with a few dedicated phased array and mechanical tracking radars, dedicated ground-based electro-optical telescopes. and dedicated space-based optical telescopes. Several of the SSN sensors are located outside of the continental United States and some of those are operated by NATO allies.

For tracking objects in LEO, the SSN originally contained elements of the Ballistic Missile Early Warning System (BMEWS) radars at Clear Air Force Station in Alaska, Thule Air Force Base in Greenland, and Royal Air Force Fylingdales in the United Kingdom. Those radars have been replaced by modern phased array systems. The SSN also contains radars that are part of the Precision Acquisition Vehicle Entry Phased Array Warning System (PAVEPAWS) system developed in the 1980s and currently located at Cape Cod Air Force Station in Massachusetts and Beale Air Force Base in California. The network also contains radars developed for missile defense, such as the Perimeter Acquisition Radar Attack Characterization System (PARCS) radar originally created for the Safeguard ABM system at Cavalier Air Force Station in North Dakota and the Cobra Dane radar at Eareckson Air Station in the Aleutian Islands. A dedicated phased array radar for space surveillance is in operation at Eglin Air Force Base in Florida.

The SSN also contains multiple radar and optical sensors that can be used to track objects out to GEO. Major sites include radars at the Lincoln Space Surveillance Complex near Boston, Massachusetts, and the Reagan Test Site on Kwajalein Atoll in the South Pacific, along with optical telescopes at the USAF Maui Optical and Supercomputing observatory in Hawaii.

In 2020, L3Harris won a 10-year, $1.2 billion contract for the creation of MOSSAIC (maintenance of space situational awareness integrated capabilities).[493] This new contract expands the previous scope of work, which prior had focused on the USAF's Ground-based Electro-Optical Deep Space Surveillance System (three radars that track objects in geostationary orbits), to support SSA centers in California, Colorado, and Virginia.

Three new ground-based radars and telescopes have recently been added to the SSN. A C-band mechanical tracking radar originally located in Antigua was moved to Naval Communication Station Harold E. Holt near Exmouth, Western Australia in March 2017.[494] A large S-Band phased array fence was also constructed on Kwajalein Atoll, which is anticipated to be able to track small space objects down to a few centimeters.[495] The USAF envisioned creating additional Space Fence sites in the future but no funding has yet been made. Finally, the Space Surveillance Telescope (SST), a 3.5-meter telescope originally developed by DARPA, has also been moved to Naval Communication Station Holt in Western Australia and will be jointly operated by the USAF's 21st Space Wing and the Royal Australian Air Force.[496] It imaged its first objects in March 2020 and is anticipated to be fully operational by 2022.[497]

In addition to the ground-based sensors, the U.S. SSN also includes multiple space-based optical sensors. The Space-Based Space Surveillance (SBSS) satellite is in LEO and has a large, gimbled telescope that can track space objects in higher orbits.[498] The Canadian Sapphire satellite is a smaller satellite in a similar orbit that also contributes to the SSN.[499] The USSF also operates the four GSSAP satellites in GEO, which can provide up-close imaging, characterization and intelligence (See U.S. Co-Orbital ASAT; section 3.1). ORS-5 (or SensorSat) was launched in 2017 and became operational in 2019.[500] It keeps an eye on GEO from an altitude of 372 miles.[501] TDO-2 was launched in March 2020 and is intended to provide space domain awareness for the USSF by using lasers to get range data on space objects, as well as allow for optical calibration options.[502] A classified space-based SSA system called "SILENT BARKER" is being jointly developed by the USSF and the NRO and is scheduled to be launched in 2022.[503]

493 Sandra Erwin, "L3Harris Wins $1.2 billion Contract to Maintain, Upgrade Space Surveillance Systems," SpaceNews, Februar

494 Steve Kotecki, "C-band Radar Reaches Full Operational Capability in Australia," Peterson Air Force Base, March 15, 2017, https://www.peterson.af.mil/News/Article/1114478/c-band-radar-reaches-full-operational-capability-in-australia/

495 Nathan Strout, "New Space Radar Likely to go Online Later This Month," C4ISRNET, February 3, 2020, https://www.c4isrnet.com/battlefield-tech/space/2020/02/03/new-space-radar-likely-to-go-online-this-month/.

496 Sandra Erwin, "U.S. Space Force Deploying Surveillance Telescope In Australia," SpaceNews, April 23, 2020, https://spacenews.com/u-s-space-force-deploying-surveillance-telescope-in-australia/.

497 "Joint US-Australian Space Surveillance Telescope To Be Improved," Australian Defence Magazine, July 16, 2020, https://www.defense.gov/Portals/1/Interactive/2018/11-2019-Missile-Defense-Review/The%202019%20MDR_Executive%20Summary.pdf

498 "Space-Based Space Surveillance," Air Force Space Command, March 22, 2017, https://www.afspc.af.mil/About-Us/Fact-Sheets/Article/249017/space-based-space-surveillance-sbss/

499 Mike Gruss, "Canada's Sapphire Satellite Begins Operations," SpaceNews, January 31, 2014, https://spacenews.com/39343canadas-sapphire-satellite-begins-operations/

500 "SMC Sets New Standard Of Success For Acquisition And Operations Of Sensorsat," SMC Public Affairs News Release, October 9, 2019, https://www.afspc.af.mil/News/Article-Display/Article/1985934/smc-sets-new-standard-of-success-for-acquisition-and-operations-of-sensorsat/.

501 Joseph Trevithick, "Space Force Has A Unit Dedicated To Orbital Warfare That Now Operates The X-37B Spaceplane," TheDrive.com, October 30, 2020, https://www.thedrive.com/the-war-zone/37361/space-force-has-a-unit-dedicated-to-orbital-warfare-that-now-operates-the-x-37b-spaceplane.

502 Nathan Strout, "The Space Force is adding another satellite to its first launch," C4ISRNET, March 10, 2020, https://www.c4isrnet.com/battlefield-tech/space/2020/03/11/the-space-force-is-adding-another-satellite-to-its-first-launch/.

503 Theresa Hitchens, "EXCLUSIVE: NRO, SPACECOM Craft CONOPS For War In Space," Breaking Defense, May 4, 2020, https://breakingdefense.com/2020/05/exclusive-nro-spacecom-craft-conops-for-war-in-space/.

In April 2019, the head of the Space Development Agency announced they were exploring architectures for extending SSA out to cislunar space.[504] AFRL's Space Vehicles Directorate is also considering what it calls "xGEO" orbits, those beyond GEO out to cislunar space, with the goal of getting SDA from GEO to past the Moon.[505] AFRL announced a project in September 2020 called "Cislunar Highway Patrol System," or CHPS, which is planned to help detect and track objects from GEO to the Moon by improving sensor technologies and algorithms needed for tracking objects.[506]

The data from the SSN sensors is collated and processed by the 18th Space Control Squadron, located at Vandenberg Air Force Base in California.[507] The mission was originally done by the 1st Space Control Squadron in Cheyenne Mountain Air Force Station in Colorado, but was moved to Vandenberg in 2007 as part of the creation of the Joint Space Operations Center (JSpOC), although much of the communications and data is still routed through Cheyenne Mountain. JSpOC became the Combined Space Operations Center (CSPoC) in July 2018 to improve interoperability with allies and commercial partners.[508] An alternate command center is located in Dahlgren, Virginia, at what used to be the control facility for the Naval Space Surveillance Fence. A significant portion of the satellite catalog maintained by the 18th SPCS and SSA analysis products such as conjunction assessments and re-entry predictions are made publicly available on the Space Track website.[509] Efforts to improve the software and computer systems used by the 18th SPCS have run into long-standing problems and delays.[510]

A new facility, originally called the 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.[511] A main function of the NSDC is to leverage military and commercial SSA capabilities to detect and characterize attacks on U.S. national security satellites.[512]

Since 2010, the United States military has actively worked to sign more than 100 SSA data sharing agreements with other countries, commercial satellite operators, and international non-governmental organizations.[513] The primary purpose of these agreements is to enable the U.S. military to share more data and analysis with other entities than what is publicly available on the Space Track website. In some cases, the agreements allow for two-way exchange of SSA data between the parties. To date, the U.S. military has signed SSA agreements with 25 countries; Australia, Belgium, Brazil, Canada, Chile, Denmark, Finland, France, Germany, Israel, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Peru, Poland, Republic of Korea, Romania, Spain, Thailand, the United Arab Emirates, and the United Kingdom.[514]

The United States has significant space weather capabilities that are provided by the USAF, the National Oceanographic and Atmospheric Administration (NOAA), and NASA. NOAA operates the National Space

504 Theresa Hitchens, "SDA's Kennedy: Cislunar Space the Next Military Frontier," Breaking Defense, April 17, 2019, https://breakingdefense.com/2019/04/sdas-kennedy-cislunar-space-the-next-military-frontier/.

505 Theresa Hitchens, "AFRL Targets Space Ops In New Orbits," Breaking Defense, June 5, 2020, https://breakingdefense.com/2020/06/afrl-to-demo-ops-in-nontraditional-orbits-for-space-force/.

506 Sandra Erwin, "Air Force Research Laboratory Announces New Space Experiments," Space News, Sept. 2, 2020, https://spacenews.com/air-force-research-laboratory-announces-new-space-experiments/.

507 "18th Space Control Squadron," Peterson Air Force Base, August 6, 2018, https://www.peterson.af.mil/About/Fact-Sheets/Display/Article/1060346/18th-space-control-squadron/.

508 "Combined Space Operations Center Established At Vandenberg AFB," Joint Force Space Component Command Public Affairs, Joint Force Space Component Command Public Affairs, Air Force Space Command, July 18, 2018, https://www.afspc.af.mil/News/Article-Display/Article/1579285/combined-space-operations-center-established-at-vandenberg-afb/.

509 Anyone can sign up for an account at https://space-track.org as long as they sign a user agreement.

510 Cristina Chaplain, "Space Command and Control: Comprehensive Planning and Oversight Could Help DOD Acquire Critical Capabilities and Address Challenges," U.S. Government Accountability Office, October 2019, https://www.gao.gov/assets/710/702424.pdf

511 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/.

512 Sandra Erwin, "Air Force Eyes Commercial Options to Gain Intelligence on Space Threats," SpaceNews, September 18, 2018, https://spacenews.com/air-force-eyes-commercial-options-to-gain-intelligence-on-space-threats/

513 Karen Singer, "100th Space Sharing Agreement Signed, Romanian Space Agency Joins," United States Strategic Command, April 29, 2019, https://www.af.mil/News/Article-Display/Article/1828045/100th-space-sharing-agreement-signed-romania-space-agency-joins/

514 Sandra Erwin, "U.S. Space Command signs space data sharing agreement with Peru," Space News, May 20, 2020, https://spacenews.com/u-s-space-command-signs-space-data-sharing-agreement-with-peru/.

Weather Prediction Center (SWPC) that collates data from a wide variety of satellites operated by NASA, the USSF, and international partners. In 2015, the Obama Administration issued the Space Weather Strategy and Action plan, which outlined the implementation approach for improving space weather capabilities.[515] An updated version was issued by the Trump Administration in 2019.[516]

MILITARY UTILITY

The United States possesses sophisticated SSA capabilities that allow it to track, identify, and characterize nearly all objects bigger than 10 centimeters in Earth orbit. While the U.S. SSN possess shortcomings in geographic coverage of LEO due to its northern location, the United States is actively working to close those gaps by deploying additional sensors to the Southern Hemisphere. Although the United States has never publicly acknowledged an explicit link between its SSA capabilities and offensive counterspace programs, it likely maintains the ability to effectively detect, track, characterize, and target any adversary national security satellites.

3.6 – U.S. COUNTERSPACE POLICY, DOCTRINE, AND ORGANIZATION

ASSESSMENT

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).

The United States is undergoing a major reorganization of its military space activities as part of a renewed focus on space as a warfighting domain. 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." This rhetoric has been accompanied by a renewed focus on reorganizing national security space structures and increasing the resilience of space systems. This has culminated in the reestablishment of U.S. Space Command (USSPACECOM) and the creation of the U.S. Space Force (USSF), which assumed the responsibilities of U.S. Strategic Command for space warfighting and Air Force Space Command (AFSPC) for operating, training, and equipping of space forces, respectively. To date, the mission of these new organizations is a continuation of previous military space missions, although some have advocated for expanding their focus to include cislunar activities and space-to-ground weapons. It is possible that

[515] "National Space Weather Action Plan," National Science and Technology Council, October 2015, https://www.sworm.gov/publications/2015/swap_final__20151028.pdf

[516] "National Space Weather Strategy and Action Plan," Office of Science and Technology Policy, March 2019, https://aerospace.org/sites/default/files/2019-03/Natl%20Space%20Weather%20Strategy%20Mar19.pdf

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. There are recent budget proposals to conduct research and development of space-based missile defense interceptors and DEW that could have latent counterspace capabilities. The United States also continues to hold annual space wargames and exercises that increasingly involve close allies and commercial partners.

SPECIFICS

U.S. 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.[517] 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.[518] 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 Trump Administration in December 2020, states, “Purposeful interference with space systems, including supporting infrastructure, will be considered an infringement of a nation's rights. Consistent with the defense of those rights, the United States will seek to deter, counter, and defeat threats in the space domain that are hostile to the national interests of the United States and its allies. Any purposeful interference with or an attack upon the space systems of the United States or its allies that directly affects national rights will be met with a deliberate response at a time, place, manner, and domain of our choosing.”[519]

[517] 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.

[518] National Security Decision Memorandum-345, January 18, 1977; Presidential Directive/NSC-37, May 11, 1978.

[519] “National Space Policy of the United States of America,” The White House, December 9, 2020, p. 4, https://web.archive.org/web/20201209213138/https://www.whitehouse.gov/wp-content/uploads/2020/12National-Space-Policy.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 historical doctrines existed on space operations: an Air Force doctrine developed by AFSPC;[520] and a joint doctrine developed by United States Strategic Command.[521] The most recent publicly available versions of these doctrines are August 2018 and October 2020, respectively. The October 2020 update to the joint doctrine reintroduced the role of USSPACECOM, realigned space capabilities with existing joint warfighting functions, added details on space threats and threat mitigation.

Under current doctrine, the U.S. military considers USSPACECOM to be a geographic combatant command with an area of responsibility of everywhere higher than 100 kilometers above the Earth. Counterspace operations fall under Space Control, which includes offensive space control and defensive space control operations to ensure freedom of action in space and achieve space superiority.[522] Threats to space systems are mitigated through space mission assurance, which includes defensive operations, reconstitution, resilience, disaggregation, distribution, diversification, protection, proliferation, and deception. Deterrence, by denying an adversary benefits and displaying the resources and resolve to respond, is critical for deterring attacks on space systems.

Offensive space control (OSC) operations consist of offensive operations conducted for space negation, where negation involves measures to deceive, disrupt, deny, degrade, or destroy adversary space systems or services. U.S. OSC operations could employ reversible and/or nonreversible means. Defensive space control (DSC) operations consist of all active and passive measures taken to protect friendly space capabilities from attack, interference, or hazards. Active space defense Active space defense consists of actions taken to neutralize imminent space control threats to friendly space forces and space capabilities. Passive space defense consists of all other measures taken to minimize the effectiveness of on-orbit and terrestrial threats to friendly space forces and friendly space capabilities, including camouflage, evasion, dispersal, and hardening.

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),[523] which concluded there was a need to identify threats in space, be able to withstand aggressive counterspace programs, and counter adversary space capabilities.[524] 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 defend itself in space.[525, 526] 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.[527, 528]

520 “Counterspace Operations,” Annex 3-14 Counterspace Operations, August 27, 2018, https://www.doctrine.af.mil/Doctrine-Publications/AFDP-3-14-Counterspace-Ops/

521 Joint Publication 3-14: Space Operations, October 26, 2020, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14ch1.pdf.

522 Ibid. pg I-4.

523 Dyke Weatherington, testimony before the House Committee on Armed Forced, Strategic Forces Subcommittee, March 25, 2015, p.3, https://docs.house.gov/meetings/AS/AS29/20150325/103106/HHRG-114-AS29-Wstate-WeatheringtonD-20150325.pdf

524 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.

525 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/.

526 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/.

527 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.

528 “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/

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.[529,530] 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.[531]

U.S. Space and Counterspace Organization — This shift in rhetoric has been accompanied by changes to the national security space organization. The U.S. Congress had criticized the USAF for its handling of space programs and forced a debate over reorganizing national security space, potentially by creating a separate entity such as a Space Corps.[532] Former President Donald Trump added further impetus to this debate by making a surprise call in June 2018 for the creation of a separate Department of the Space Force.[533] Ultimately, the Trump Administration released Space Policy Directive (SPD)-4 in February 2019, which settled on calling for a more moderate approach that combines resurrecting USSPACECOM to take over space warfighting duties from USSTRATCOM[534] and the creation of a Space Force as a new military service within the Department of the Air Force.[535]

Part of the renewed U.S. focus on space warfighting includes closer ties with allies and commercial partners. Historically, the U.S. national security space sector has been very isolated from other countries and commercial entities, even more so than the cyber and intelligence sector. Since 2010, there have been numerous efforts to bridge this gap. The 2010 edition of the then-biennial Schriever wargame exercised the concept of a Combined Space Operations Center (CSpOC) that integrated allies and commercial partners into the decision-making during the scenarios.[536] Following the wargame, USSTRATCOM began working on plans to make the CSpOC a reality. Initially, it was brought to life in the form of the Combined Space Operations (CSpO) concept, which involved each partner creating their own national space operations center and establishing lines of communication and coordination between them. The founding partners were the United States, Australia, Canada, and the United Kingdom.[537] New Zealand was added in 2015 and France and Germany joined in 2019.[538]

529 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.

530 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.

531 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.

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

533 Katie Rogers, "Trump orders establishment of Space Force as sixth military branch," The New York Times, June 18, 2018, https://www.nytimes.com/2018/06/18/us/politics/trump-space-force-sixth-military-branch.html.

534 The White House, "Text of a memorandum from the President to the Secretary of Defense regarding the establishment of the United States Space Command", Whitehouse.gov, December 18, 2018, https://aerospace.org/sites/default/files/2019-01/US%20Space%20Command%20memo%2018Dec18.pdf

535 The White House, "Text of Space Policy Directive-4: Establishment of the United States Space Force", Whitehouse.gov, February 19, 2019, https://media.defense.gov/2019/Mar/01/2002095015/-1/-1/1/SPACE-POLICY-DIRECTIVE-4-FINAL.PDF

536 Larry James, "The Challenge of Integration: Lessons from Schriever Wargame 2010", High Frontier, Vol 7 No 1, November 2010, https://www.afspc.af.mil/Portals/3/documents/HF/AFD-101116-028.pdf

537 Cheryl Pellerin, "Stratcom, DoD Sign Space Operations Agreement with Allies," Defense.gov, September 23, 2014, https://www.defense.gov/Explore/News/Article/Article/603303/stratcom-dod-sign-space-operations-agreement-with-allies/

538 USSPACECOM Public Affairs, "Combined Space Operations Initiative Welcomes France and Germany," United States Space Command, February 12, 2020, https://www.spacecom.mil/MEDIA/NEWS-ARTICLES/Article/2083368/combined-space-operations-initiative-welcomes-france-and-germany/

In addition to maintaining their own national centers, U.S. Strategic Command's JSpOC was renamed the CSpoC and included CSpO exchange officers and a Commercial Integration Cell (CIC).[539]

On March 23, 2018, the Trump Administration issued a new National Space Strategy (NSS) that echoed similar themes as expressed at the end of the Obama Administration but with more aggressive rhetoric.[540] The strategy called for U.S. preeminence in space and peace through strength by promoting four pillars: transforming to more resilience space architectures; strengthening space deterrence and warfighting architectures; improving foundational capabilities, structures, and processes; and fostering conducive domestic and international environments. The Strategy also publicly states for the first time that the United States believes space is a warfighting domain.

The aggressive rhetoric from the Trump Administration increased in the latter half of 2018 and throughout 2019, but it is unclear if the rhetoric reflects actual U.S. policy. In various speeches and rallies promoting the USSF, President Trump called for the United States to "dominate" space. Vice President Mike Pence reiterated this language in a speech at Johnson Space Center, stating that the Trump Administration was taking steps to "ensure American national security is as dominant in space as it is here on Earth".[541] In his remarks during the signing ceremony for establishing the USSF, President Trump said the United States was developing "a lot of new defensive weapons and offensive weapons" that they were now "going to take advantage of" with the USSF.[542] Yet official U.S. policy statements on space security issues, or at least the public ones, continue to reflect a more moderate tone and do not explicitly outline the development of new offensive space weapons.[543]

USSPACECOM was officially re-established as the eleventh combatant command on August. 29, 2019, in a ceremony at the White House Rose Garden.[544] Gen. Jay Raymond was named as Commander of USSPACECOM, which was established as a geographic combatant command with authority for all U.S. military operations above 100 km altitude.[545] The mission of USSPACECOM is to deter aggression and conflict, defend U.S. and allied interests, deliver space combat power, and develop ready and lethal joint warfighters.[546] Initially, USSPACECOM will consist of two subordinate commands, each of which is comprised of several already existing commands and operations centers. Combined Force Space Component Command (CFSCC) plans, integrates, conducts, and assesses global space operations and consists of the CSpOC at Vandenberg, Air Force Base, California; the Missile Warning Center at Cheyenne Mountain Air Force Station, Colorado; the Joint Overhead Persistent Infrared Center at Buckley Air Force Base, Colorado; and the Joint Navigation Warfare Center located at Kirtland Air Force Base, New Mexico.[547] The Joint Task Force Space Defense (JTF-SD) conducts space superiority operations with allies and partners and includes the NSDC at Schriever Air Force Base in Colorado.[548]

539 "Combined Space Operations Center / 614th Air Operations Center," U.S. Strategic Command, July 2018, https://www.stratcom.mil/Portals/8/Documents/CSpOC_Factsheet_2018.pdf

540 The White House, "President Donald J. Trump is unveiling an America first National Space Strategy," Whitehouse.gov, March 23, 2018, https://aerospace.csis.org/wp-content/uploads/2018/09/Trump-National-Space-Strategy.pdf

541 Tal Axelrod, "Pence: Trump Administration's national security will be as 'dominant' in space as it is on Earth," The Hill, August 23, 2018, https://thehill.com/homenews/administration/403316-pence-trumps-national-security-will-be-as-dominant-in-space-as-it-is.

542 The White House, "Remarks by President Trump at Signing Ceremony for Space Policy Directive-4 (Space Policy Comments Excerpt)", SpaceRef.com, February 19, 2019, http://spaceref.com/news/viewsr.html?pid=52251.

543 For example, the formal strategy proposal for the Space Force does not include the word "dominate". See https://media.defense.gov/2019/Mar/01/2002095012/-1/-1/1/UNITED-STATES-SPACE-FORCE-STRATEGIC-OVERVIEW.PDF

544 Jim Garamone, "Pentagon Rolls Out Space Command," U.S. Department of Defense, August 29, 2019, https://www.defense.gov/Explore/News/Article/Article/1948420/pentagon-rolls-out-space-command/.

545 Theresa Hitchens, "SPACECOM to Write New Ops War Plan: 100km and Up," Breaking Defense, September 16, 2019, https://breakingdefense.com/2019/09/spacecom-to-write-new-ops-war-plan-100km-and-up/.

546 "United States Space Command Fact Sheet," United States Space Command, June 20, 2018, https://www.spacecom.mil/Portals/32/USSPACECOM%20Fact%20Sheet%2018Jun20.pdf?ver=2020-06-18-155219-363

547 Theresa Hitchens, "Raymond's First SPACECOM Move: Two New Subcommands and Their Leaders," Breaking Defense, August 30, 2019, https://breakingdefense.com/2019/08/raymonds-first-spacecom-move-two-new-subcommands-and-their-leaders/.

548 Ibid.

The USSF was formally created on December 20, 2019, with President Trump's signing of the Fiscal Year 2020 National Defense Authorization Act.[549] The signing follows an intense debate between the House, Senate, and White House throughout much of 2019. The compromise signed into law more closely resembles the Space Corps idea pushed by the House in 2017 than the separate department President Trump wanted in June 2018.[550] The USSF is a separate military service with independent powers to train, equip, and operate, but exists within the Department of the Air Force to reduce overhead. Initially, the USSF consists only of members of the USAF and is being slowly stood up over an 18-month period, beginning by re-designating AFSPC as the USSF. One year after its creation, the USSF has about 2000 personnel transferred into it and expects to eventually have 16,000 members.[551] The commander of the USSF, initially Gen. Raymond, will be the Chief of Space Operations and serve on the Joint Chiefs of Staff. The Secretary of the Air Force has also been tasked to create a Space Force Acquisitions Council, which will assume responsibility for all military space acquisitions by Fiscal Year 2022.

The top-level organization of the USSF was announced in July 2020, with training in USSF to be overseen by the Space Training and Readiness Delta Provisional, which will eventually evolve into the Space Training and Readiness Command, or STARCOM; operations over seen by Space Operations Command; and acquisitions overseen by Space Systems Command.[552] While the Biden administration has not made space a prominent policy issue in its first few months in office, White House spokesperson Jen Psaki said in February 2021 of the USSF, "They absolutely have the full support of the Biden administration," and that "We are not revisiting the decision to establish the Space Force."[553]

USSF released its Space Capstone Publication Spacepower in August 2020, articulating its initial spacepower theories and doctrines.[554] Regarding offensive counterspace, the document statues "Offensive operations target an adversary's space and counterspace capabilities, reducing the effectiveness and lethality of adversary forces across all domains. Offensive operations seek to gain the initiative and may neutralize adversary space missions before they can be employed against friendly forces. Offensive operations are not limited to adversary counterspace systems and can also target the full spectrum of an adversary's ability to exploit the space domain, which includes targets in the terrestrial and cyber domains."[555]

In May 2020, Gen. John Raymond signed the first operations order as Commander of USSAPCECOM for Operation Olympic Defender (OOD), USSPACECOM's plan to protect U.S. and allied satellites during a conflict.[556] OOD was created by USSTRATCOM in 2013 and opened up for ally participation in 2018.[557] The United Kingdom became the first ally to join OOD in July 2019.[558]

549 Leonard David, "Trump Officially Establishes US Space Force with 2020 Defense Bill Signing," Space.com, December 21, 2019, https://www.space.com/trump-creates-space-force-2020-defense-bill.html

550 Kaitlyn Johnson, "Congress Approved the Space Force. Now What?," Center for Strategic and International Studies, December 19, 2020, http://aerospace.csis.org/wp-content/uploads/2019/12/NDAA-Space-Force.2.pdf

551 Joe Pappalardo, "The Space Force Turns One," Air & Space Magazine, December 2020, https://www.airspacemag.com/military-aviation/space-force-turns-one-180976342/.

552 Brian W. Everstine, "Space Force Announces Significant Reorganization," Air Force Magazine, July 24, 2020, https://www.airforcemag.com/space-force-organizations-take-shape-as-selection-boards-meet/.

553 Darlene Superville, "White House Offers 'Full Support' For Trump-Era Space Force," Associated Press, Feb. 3 2021, https://apnews.com/article/joe-biden-politics-jen-psaki-e8007099b8b457dd84fa4def85ac30e0.

554 Sandra Erwin, "U.S. Space Force Unveils Doctrine Explaining Its Role In National Security," Space News, Aug. 10, 2020, https://spacenews.com/u-s-space-force-unveils-doctrine-explaining-its-role-in-national-security/.

555 Space Capstone Publication: Spacepower. Doctrine for Space Forces, U.S. Space Force, June 2020, https://www.spaceforce.mil/Portals/1/Space%20Capstone%20Publication_10%20Aug%202020.pdf

556 Theresa Hitchens, "'Major Milestone' as Allies Join SPACECOM's War Plan," BreakingDefense.com, May 21, 2020, https://breakingdefense.com/2020/05/major-milestone-as-allies-join-spacecoms-war-plan/.

557 Hitchens, May 21, 2020, ibid.

558 "USSPACECOM releases first formal order to execute multinational space operations," USSPACECOM, May 21, 2020, https://www.spacecom.mil/MEDIA/NEWS-ARTICLES/Article/2194150/usspacecom-releases-first-formal-order-to-execute-multinational-space-operations/.

The NRO and USSPACECOM announced in May 2020 that they were working on a shared "playbook" for how to protect military and intelligence satellites during a conflict as part of a joint concept of operations (CONOPS).[559] According to the NRO's deputy director, this is intended to "strengthen and synchronize our defensive operations" and to clarify who defends what.[560] The new head of USSPACECOM, Army Gen. James Dickinson, released his "Commander's Strategic Vision" in January 2021.[561] Its goal is to set the foundations for future organizational documents like planning guidance, operational plans, and campaign plans[562]. General Dickinson defined USSPACECOM's mission as conducting "operations in, from and to space to deter conflict, and, if necessary, defeat aggression, deliver space combat power for the Joint/Combined Force and defend U.S. vital interests with allies and partners."[563] To meet that mission, the document called for establishing space superiority and providing "space combat power by fully integrating offensive and defensive operations alongside our longstanding allies and partners."[564]

The latest version of the Unified Command Plan (UCP 2020), which outlines the relationships between the combatant commands, was signed by Trump in January 2021.[565] This document elucidated USSPACECOM's roles and responsibilities compared to the other combat commands, and charged USSPACECOM with decision-making authority to determine which targets will be tracked via space assets and who has priority for using communications satellites during conflict.[566] It also gave USSPACECOM some new responsibilities: "global sensor manager" and "global satcom bandwidth manager."[567]

U.S. Counterspace Budget and Exercises — 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,[568] and it increased again in FY18 to $68.38 million.[569] Nearly all of the increase 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 USAF and Air National Guard units.[570]

559 Theresa Hitchens, "EXCLUSIVE: NRO, SPACECOM Craft CONOPS For War In Space," Breaking Defense, May 4, 2020, https://breakingdefense.com/2020/05/exclusive-nro-spacecom-craft-conops-for-war-in-space/.

560 Hitchens, May 4, 2020, ibid.

561 Never a Day Without Space: Commander's Strategic Vision, USSPACECOM, January 2021, https://www.spacecom.mil/Mission/Commanders-Strategic-Vision/

562 Theresa Hitchens, "SPACECOM's New Vision Targets 'Space Superiority'," Breaking Defense, Jan. 28 2021, https://breakingdefense.com/2021/01/spacecoms-new-vision-targets-space-superiority/.

563 Commander's Strategic Vision, January 2021, p. 6.

564 Commander's Strategic Vision, January 2021, ibid.

565 Hitchens, Jan. 28, 2021, ibid.

566 Theresa Hitchens, "Exclusive: Milley To OK New Unified Command Plan; Defines SPACECOM's Roles," Breaking Defense, Aug. 26, 2020, https://breakingdefense.com/2020/08/exclusive-milley-to-sign-new-unified-command-plan-defines-spacecoms-roles/.

567 Hitchens, Aug. 26, 2020, ibid.

568 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, https://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

569 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.

570 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.

The FY19 budget for these same programs decreased to $26.7 million.[571] 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.[572]

In March 2019, the Pentagon released its FY 2020 budget request, which listed "investing in the emerging space and cyber warfighting domains" as a major priority. While there was an overall increase of 22% in requested funding for military space programs, space control and counterspace programs saw a 46% decrease in requested funding.[573] The majority of this change was a shift of an AF TENCAP program to another budget line. Other programs such as CCS, BOUNTY HUNTER, and Offensive Counterspace C2 continue at modest funding levels.[574] In February 2020, the Pentagon released its FY 2021 budget request, which included an increase of 36% in funding for counterspace programs, mainly due to accelerating the development of additional CCS systems. The Pentagon also asked for $77M in overseas contingency operations funding to support counterspace operations.[575]

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 2018 Schriever Wargame looked at a scenario involving a notional peer space and cyberspace competitor in the U.S. Indo-Pacific Command (USINDOPACOM) Area of Responsibility and included participation from Australia, Canada, France, Germany, Japan, New Zealand, and the United Kingdom.[576] 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.[577] The USAF says it expects to hold future Space Flags biannually. Space Flag 20-1 was held at the Boeing Virtual Warfare Center in St. Louis, Missouri, on December 20, 2019.[578] The USAF's Advanced Battle Management System (ABMS) held an exercise in April 2020 that was intended to support USSPACECOM as its space assets came under simulated attack.[579]

571 Exhibit R-2, RDT&E Budget Item Justification: FY 2018 Air Force, Vol. 2, Program Element: PE 1206421F / Counterspace Systems, May 2018: p. 751, https://www.saffm.hq.af.mil/Portals/84/documents/FY19/RDT_E/Air%20Force%20Research%20Development%20Test%20and%20Evaluation%20Vol%20II%20FY19%20v2.pdf#page=751.

572 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.

573 Velos, PB20 budget summary document, March 20, 2019, https://files.constantcontact.com/bd3dd1d9401/1fd41231-1164-4c82-8d0e-5c30be4680dc.pdf.

574 Exhibit R-2, RDT&E Budget Line Item Justification: PB2020 Air Force, Vol. 2, Program Element 1206421F / Counterspace Systems, March 2019, p. 997, https://www.saffm.hq.af.mil/Portals/84/documents/FY20/RDTE/FY20_PB_RDTE_Vol-II.PDF?ver=2019-03-18-153506-683#[page=997.

575 Valerie Insinna "Space Force Asks for $15B in First Budget Request," DefenseNews, February 10, 2020, https://www.defensenews.com/smr/federal-budget/2020/02/10/the-space-forces-15-billion-budget-for-fy21-shows-a-service-in-transition/

576 Tracy Cozzens, "Schriever Wargame 2018 concludes," GPS World, October 19, 2018, https://www.gpsworld.com/schriever-wargame-2018-concludes/.

577 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/.

578 Tyler Whiting, "Space-superiority Exercise, Space Flag, Successfully Completed on U.S. Space Force Birthday," Parabolic Arc, January 19, 2020, http://www.parabolicarc.com/2020/01/19/space-superiority-exercise-space-flag-successfully-completed-on-u-s-space-force-birthday/

579 Theresa Hitchens, "Attack On US Satellites Focus Of Next ABMS Test: Goldfein," BreakingDefense.com, March 3, 2020, https://breakingdefense.com/2020/03/attack-on-us-satellites-focus-of-next-abms-test-goldfein/.

04 France

ASSESSMENT

While France has long had a space program, as well as military satellites, it was not until recently that France had an explicit focus on offensive and defensive counterspace activities. The major change occurred in July 2019 with the release of the first French Space Defense Strategy, which elevated French military space efforts and control of French military satellites. The French Space Defense Strategy focuses on two main areas: to improve space situational awareness around French space assets and provide them with some form of an active defense against threats. While some French officials suggested machine guns and laser cannons on satellites, the actual plan calls for ground-based lasers for dazzling and space-based inspection satellites.

SPECIFICS

DA-ASAT Technologies — There are no known plans for France to have a DA-ASAT capability at this time. France does have a jointly fielded missile defense system with Italy called SAMP/T (Surface-to-Air Missile Platform/Terrain); however, its interception altitude is at best 120 km, and is thus not of much military utility as an ASAT.[580]

Co-Orbital Technologies — In July 2019, when announcing France's interest in developing active counterspace capabilities, French Minister of Defense Florence Parly did reportedly offer the option of including machine guns on satellites that would theoretically target enemy satellites' solar panels.[581] This was part of a larger discussion about how "our allies and adversaries are militarising space...we need to act."[582] However, in private discussions with French officials, this was clarified as having been a poorly-used metaphor. Orbital mechanics severely limits the utility of projectile weapons in orbit.

Electronic Warfare — While France has terrestrial-based EW capabilities, there are scant details available in the public domain and it is unclear how effective or operational they are against space capabilities.

Directed Energy — In July 2019, French Minister of Defense Florence Parly indicated the potential for placing lasers on satellites with the goal of protecting them from attack. "If our satellites are threatened, we intend to blind those of our adversaries...We reserve the right and the means to be able to respond: that could imply the use of powerful lasers deployed from our satellites or from patrolling nano-satellites."[583] These lasers would "dazzle those who would be tempted to approach too close." [584] Minister Parly said that by 2025, the first capabilities under her strategy should be ready, with the completion being achieved by 2030.[578]

It is unclear whether these are meant to be destructive laser weapons or those used as countermeasures against the targeting systems of an attacker. A nanosatellite is very unlikely to have sufficient on-board power to generate a destructive laser, although it may be possible to have lower power directed energy systems that could be used to blind, dazzle, or confuse electro-optical targeting systems of approaching

580 Missile Defense Advocacy Alliance, "SAMP/T Air Defense System (France & Italy)," https://missiledefenseadvocacy.org/defense-systems/sampt-air-defense-system/.

581 Adam Plowright and Daphne Benoit, "France to develop anti-satellite laser weapons: minister," Phys.org, July 25, 2019, https://phys.org/news/2019-07-france-unveil-space-defence-strategy.html.

582 Ibid.

583 Plowright and Benoit, ibid.

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

585 Taylor Mahlandt, "France is Getting Serious About Its 'Space Command," SpaceWatch Global, August 1, 2019, https://spacewatch.global/2019/09/cnes-supports-french-armed-forces-in-implementing-military-space-strategy/

co-orbital ASATs or inspection satellites. These systems could operate in a similar manner to the directional infrared countermeasures systems mounted on some modern aircraft to confuse or jam infrared seekers on anti-aircraft missiles. However, successfully aiming such a laser at an approaching satellite or interceptor is a non-trivial challenge.

Space Situational Awareness — France's Space Command is charged with coordinating SSA for the country as a whole. It operates the Grand Réseau Adapté à la Veille Spatiale (GRAVES) radar, which can see objects with radar cross sections down to 1 meter at an altitude of 400-1000 km.[586] France also has three SATAM C-band radars which are not primarily SSA sensors but do have a secondary mission to track space debris.[587] Another asset which contributes to French SSA capabilities (but does so in the capacity of it being its secondary mission) is the Bâtiment d'Essaiset de Mesures (BEM) Monge tracking ship.[588] France also has the SPOC (Systéme Probatoire d'Observation du Ciel) telescope, which can do initial orbit determinations, and the TAROT system of two 25-centimeter telescopes, which – along with the ROSACE telescope – can track objects at GEO.[589] All of these capabilities contribute to France's Centre Opérationnel de Surveillance Militaire des Objets Spatiaux (COSMOS), its Military Surveillance Operational Centre of Space Objects.[590]

In her July 2019 announcement about France's interest in counterspace capabilities, French Minister of Defense Florence Parly noted that while France has some existing SSA capabilities, it wished to work with other European Union countries on shoring those up. Specifically, she said, "France has her independence and is attached to it. But she does not want to be isolated in this new zone of conflicts…I am counting particularly on Germany to become the beating heart of surveillance in space."[591] The Franco-German Space and Defence Council in 2017 approved a joint SSA project, which is hoped to be able to provide clarifying information about unfriendly or hostile actions in space.[592] The existing French GRAVES ground-based phased array radar is intended to have a follow-up capability, which, according to Parly, "must be able to detect satellites 1,500 km away that are no bigger than a shoe-box." [593] Parly also said that they plan to use Ariane Group's Geotracker network in order to capture pictures of objects in GEO.[594]

Parly also spoke about launching patroller mini-satellites by 2023 which she described as "fearsome little detectors that will be the eyes of our most valuable satellites."[595] These patroller satellites seem to be similar to the U.S. GSSAP satellites already operating in the GEO region (See U.S. Co-Orbital ASAT; section 3.1). Another capability being discussed are on-board cameras for the Syracuse military communications satellites that could alert satellites to oncoming threats so that the satellites can take defensive actions or maneuvers.[596] Again, doing so is difficult in practice given the orbital mechanics of RPO in GEO.

586 Andrea Console, "Command and Control of a Multinational Space Surveillance and Tracking Network," NATO Joint Air Power Competence Centre, June 2019, https://www.japcc.org/wp-content/uploads/JAPCC_C2SST_2019_screen.pdf, p. 33.

587 Ibid.

588 Console, ibid, p. 34.

589 Ibid.

590 Ibid.

591 Plowright and Benoit, ibid.

592 Office of the President of the French Republic, "Meeting of the French-German Defense and Security Council: conclusions (excerpt)," July 14, 2017, https://www.defense-aerospace.com/articles-view/verbatim/4/185306/conclusions-of-franco_german-defense-council.html.

593 Christina Mackenzie, "France plans to boost its self-defense posture in space," Defense News, July 26, 2019, https://www.defensenews.com/global/europe/2019/07/26/france-plans-to-boost-its-self-defense-posture-in-space/.

594 Hitchens, July 26, 2019, ibid.

595 Reporting by Sophie Louet, writing by Richard Lough, "France to launch 'fearsome' surveillance satellites to bolster space defenses," Reuters, July 25, 2019, https://www.reuters.com/article/us-france-space-defence/france-to-launch-fearsome-surveillance-satellites-to-bolster-space-defenses-idUSKCN1UK1TY.

596 Arthur Laudrain,"France's 'strategic autonomy' takes to space," IISS Military Balance Blog, August 14, 2019, https://www.iiss.org/blogs/military-balance/2019/08/france-space-strategy.

Counterspace Policy, Doctrine, and Organization — In September 2018, French Minister of Defense Florence Parly surprised some by openly calling out the Russians for using their Luch Olymp satellite to allegedly attempt to spy on France's Athena-Fidus satellite (See Russian Co-Orbital ASAT; section 2.1). She said, "It got so close that we might have imagined it was trying to intercept our communications," and commented, "Trying to listen to your neighbors is not only unfriendly. It's an act of espionage."[597] It should be noted that surveillance of this type does not violate any existing international laws.

In July 2019, French President Emmanuel Macron announced that by September 1 of that year, France would be elevating the existing Joint Space Command within the French Air Force to be a full Space Command and renaming the French Air Force to be the Air and Space Force, or the Armée de l'Air et de l'Espace. He said that this was to "ensure the development and reinforcement of our space capabilities."[598] France's Space Command (or Commandement de l'espace, CDE) is starting off with 220 people as its staff and will grow eventually to 500 when it reaches full operational capacity in 2025.[599] According to Parly, "Eventually, this command will be responsible for all our space operations, under the orders of the Chief of Staff of the Armed Forces." She noted the importance of the Ministry of Armed Forces becoming a space operator, as "If we want to be able to carry out real military space operations, we must develop autonomy of action."[600]

The French military had originally put aside 3.6 billion Euros (roughly $4 billion) to invest in its satellites from 2019-2025.[601] Parly announced in July 2019 an additional 700 million Euros for this effort.[602] This 4.3 billion Euros include funds for refreshing France's military space infrastructure (reconnaissance, signals intelligence, and communications satellites, as well as the GRAVES radar used for space surveillance). Parly also noted that France will be testing a long-range radar in face of increased missile threats.

In July 2019, France also announced its first Space Defense Strategy.[603] It has two goals: to increase and strengthen SSA in order for there to be better decision-making and to protect French and selected European space assets. This strategy is intended to be defensive in nature, with Parly noting in her July 2019 speech that this was "not an arms race."[604]

According to Parly, "active defense is not an offensive strategy, it's all about self-defense...That is, when a hostile act has been detected, characterized and attributed, to be able to respond in an appropriate and proportionate way, in conformity with the principles of international law."[605]

597 Christina Maza, "Russian Spy Satellite Tried to Steal Military Information from France, Defense Minister Says," Newsweek, September 17, 2018, https://www.newsweek.com/russian-spy-satellite-tried-steal-military-information-france-1112072.

598 Sophie Louet, Myriam Rivet and Bate Felix, "France to create space command within air force: Macron," Reuters, July 13, 2019, https://www.reuters.com/article/us-france-nationalday-defence/france-to-create-space-command-within-air-force-macron-idUSKCN1U80LE.

599 Christina Mackenzie, "French Air Force Changes Name As It Looks To The Stars," Defense News, September 15, 2020, https://www.defensenews.com/global/europe/2020/09/15/french-air-force-changes-name-as-it-looks-to-the-stars/#:~:text=In%20a%20statement%2C%20the%20Air,command%20is%20led%20by%20Brig.

600 Ibid.

601 Norimitsu Onishi, "France Nudges Europe Into Space Race, Where It Lags Behind," New York Times, July 18, 2019, https://www.nytimes.com/2019/07/18/world/europe/france-europe-space-race-apollo-11-anniversary.html.

602 Office for Science & Technology of the Embassy of France in the United States, "Defence - Space command to be created," July 30, 2019, https://www.france-science.org/Defence-Space-command-to-be.html.

603 The French Ministry for the Armed Forces, Space Defence Strategy, Report of the Space Working Group, 2019; downloaded from: https://www.defense.gouv.fr/english/actualites/articles/florence-parly-devoile-la-strategie-spatiale-francaise-de-defense.

604 Laudrain, ibid.

605 Hitchens, ibid.`

The space defense strategy noted that the renewed doctrine for military space operations will have the following four functions: "support for space capabilities, situational awareness, support for operations and action in space."[606] It also stated that a "consolidated assessment of threats affecting our capabilities" will be needed.[607] France's Defense Innovation Agency is now intended to take part in space research and development guidelines.

The strategy talks about the need to be able to respond to "unfriendly, illegal or aggressive acts, in accordance with international law."[608]
It gives the following guidelines for responses in these cases:

- in the face of an unfriendly act in space, France reserves the right to take retaliatory measures;

- in response to an unlawful act committed against it, it may take countermeasures with the sole purpose of putting an end to it, in accordance with its obligations under international law; these countermeasures will be strictly necessary and proportionate to the objective;

- in the event of armed aggression in space, France can make use of its right to self-defence."[609]

The strategy does recommend France continue to participate in multilateral fora, especially so it can "focus on behavioural standards to ensure strategic stability and avoid opportunities for misunderstandings or escalations."[610]

As part of this overhaul of France's military space capabilities, the French Ministry of Defense would now be allowed to conduct activities in space. To allow for this shift toward military space, France's National Space Law will have to go through inter-ministerial discussions to be adapted to reflect this new set-up. France's June 2008 Space Operations Act (LOS) encourages space activity to be primarily commercial and/or civil in nature.[611] It was created in order to meet France's Article 6 obligations of the 1967 Outer Space Treaty, which requires continuing supervision of national space activities. Legislation is needed to create the legal framework to allow the Minister of the Armed Forces to become the operator of all French defense satellites, instead of CNES.

[606] Space Defence Strategy, pp. 12-13.

[607] Ibid.

[608] Ibid, p. 26.

[609] Ibid, p. 27.

[610] Ibid.

[611] Philippe Clerc, "The French Space Operations Act," December 2011, https://www.iislweb.org/docs/2011_galloway/Clerc.pdf.

05 India

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.[619] 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 iterated, "India does not believe in weaponization of space. We are only talking about having the capability. There are no plans for offensive space capabilities."[620]

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 Defence (PAD) system (later to be replaced by the Prithvi Defence Vehicle, or PDV) and the Advanced Area Defence (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.[621] It was tested at night in September 2018 and was able to "successfully engage" its target.[622] The AAD was launched in March 2017 to make a successful intercept at an altitude of 15-25 km.[623] It was tested in August 2018 and successfully destroyed its target, which was surrounded by decoys.[624] In January 2020, government officials stated that the system was complete.[625] India has also negotiated a deal with Russia to buy four of its S-400 Triunf surface-to-air missile systems for $5.5 billion.[626] India's missile defense network uses the Green Pine radar, which was developed by Israel as part of its Arrow missile defense system.

On March 27, 2019, the Indian Prime Minister announced that they had successfully conducted Mission Shakti, where an interceptor launched from the Kalam Island launch complex successfully intercepted one of India's satellites at an altitude of about 300 km. The missile used was from India's indigenously developed missile defense system, a PDV MK-II, and that the satellite target was Microsat-R, which was a medium-sized (740 kg) Indian military imaging satellite launched into a low Sun-synchronous orbit in January 2019. Reportedly, the decision was made in 2017 to undertake the test, giving DRDO engineers about 20 months to ensure that the kill vehicle was ready for it.[627] In a fact sheet released about the ASAT test, the Indian government explained, "The test was done to verify that India has the capability to safeguard our space assets. It is the Government of India's responsibility to defend the country's interests in outer space," but went on to say, "We are against the weaponization of Outer Space and support international efforts to reinforce the safety and security of space-based assets."[628] After the test was held, DRDO Chair G. Sateesh Reddy told reporters that "We don't need any more tests in this orbit now," but did not rule out tests at higher orbits.[629] Minister of Defense Rajnath Singh tweeted on the

619 Ibid.

620 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.

621 "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.

622 "India Conducts Successful Interceptor Missile Test at Night," PTI, September 23, 2018, https://economictimes.indiatimes.com/news/defence/india-conducts-successful-interceptor-missile-test-at-night/articleshow/65925514.cms

623 "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.

624 Franz-Stefan Gady, "India's Advanced Air Defense Interceptor Shoots Down Ballistic Missile Target in Test," The Diplomat, August 3, 2018, https://thediplomat.com/2018/08/indias-advanced-air-defense-interceptor-shoots-down-ballistic-missile-target-in-test/

625 Snehesh Alex Philip, "India's Ballistic Missile Shield Ready, IAF & DRDO To Seek Govt Nod To Protect Delhi," The Print, January 8, 2020, https://theprint.in/defence/indias-ballistic-missile-shield-ready-iaf-drdo-to-seek-govt-nod-to-protect-delhi/345853/.

626 Rahul Bedi, "Why Is the US Saying India Could Face Sanctions for Buying Russian S-400 Missile Systems?," TheWire, January 20, 2021, https://thewire.in/security/us-india-sanctions-caatsa-s400-russia.

627 Indranil Roy, "All You Need To Know About The PDV MK-II: India's Satellite Killer," Delhi Defence Review, April 3, 2019, http://delhidefencereview.com/2019/04/03/all-you-need-to-know-about-the-pdv-mk-ii-indias-satellite-killer/. This article goes into deep detail about the interceptor

628 "Frequently Asked Questions on Mission Shakti, India's Anti-Satellite Missile test conducted on 27 March, 2019," Ministry of External Affairs, Government of India, March 27, 2019, https://www.mea.gov.in/press-releases.htm?dtl/31179/Frequently_Asked_Questions_on_Mission_Shakti_Indias_AntiSatellite_Missile_test_conducted_on_27_March_2019.

629 Snehesh Alex Philip, "DRDO Rules Out A-SAT Tests In Lower Earth Orbits, But Keeps Options Open In Higher Orbits," ThePrint, April 6, 2019, https://theprint.in/defence/drdo-rules-out-a-sat-tests-in-lower-earth-orbits-but-keeps-options-open-in-higher-orbits/217879/ .

one-year anniversary of Mission Shakti, "The success of 'Mission Shakti' proved our capability to defend the assets in outer space and made India the 4th Space Power in the world." [630]

Shortly after the test, anonymous U.S. government sources stated that they had detected an earlier failed ASAT test in February 2019 where the PDV failed thirty seconds into flight.[631] The Indian government had issued a NOTAM just before this flight and the time of the launch correlated with an overflight of Microsat-R, another indication that it was launched into orbit to be a target for an ASAT test.

TABLE 11 - INDIAN DA-ASAT TESTS IN SPACE

DATE	ASAT SYSTEM	ASAT TYPE	LAUNCH SITE	TARGET	NOTES
Feb. 12, 2019	PDV-MK II	direct ascent	Abdul Kalam island	Microsat-R	Unsuccessful intercept
Mar. 27, 2019	PDV-MK II	direct ascent	Abdul Kalam island	Microsat-R	Successful intercept, debris generated

Indian officials downplayed concerns about large amounts of debris being created by this test, stating that the test was at a low enough altitude that most of the debris would reenter in a few days, with the entirety of it coming back down within 45 days at most.[632] Microsat-R was similar in mass to the FY-1C satellite destroyed by China in January 2007, which resulted in more than 3,000 pieces of orbital debris larger than 10 cm (See Chinese Direct-Ascent ASAT; section 1.2). However, Microsat-R was at a much lower altitude when destroyed, 300 km versus 800 km for the FY-1C, meaning orbital debris generated will have a shorter lifespan. The U.S. 18th Space Control Squadron (which is charged with tracking orbital debris) tracked roughly 125 pieces of debris from this test; as of February 2020, there were still 10 pieces being tracked, and at least some pieces had been thrown to an altitude of 1000 km due to collision dynamics, as happened with the February 2008 intercept of USA 193 by the United States (see U.S. Direct-Ascent ASAT; section 3.2).

A prime motivation for the test was likely to ensure India would be grandfathered into any future ban on DA-ASAT testing. 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. Successfully demonstrating their own DA-ASAT capability might have been a political prerequisite for India to support discussions on a future ban.

630 Pradip Sagar, "A year after Mission Shakti, DRDO says it has no plans to repeat it," The Week, March 27, 2020, https://www.theweek.in/news/india/2020/03/27/a-year-after-mission-shakti-drdo-says-it-has-no-plans-to-repeat-it.html.

631 Ankit Panda, "Exclusive: India Conducted a Failed Anti-Satellite Test in February 2019," The Diplomat, March 30, 2019, https://thediplomat.com/2019/04/exclusive-india-conducted-a-failed-anti-satellite-test-in-february-2019/

632 Marco Langbroek, "Why India's ASAT Test Was Reckless: Publicly available data contradicts official Indian assertions about its first anti-satellite test," The Diplomat, April 30, 2019, https://thediplomat.com/2019/05/why-indias-asat-test-was-reckless/.

India's space vehicle launchpad is at Satish Dhawan Space Center near Sriharikota (See Satish Dhawan, page 10-14). Officials announced in August 2017 that work has begun on a second vehicle assembly building at the center that is anticipated to be completed by mid-2018.[633] 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."[634] Launches from the center are expected to increase from seven a year to 12 a year.[635]

Directed Energy — India is reportedly in the early stages of working on directed energy weapons. In August 2019, Reddy acknowledged, "We have been working in this area for the past three to four years to develop 10-kW and 20-kW" weapons.[636] However, the targets for these weapons, which are in the very early stages of development, are aerial or electronic in nature:[637] they do not appear to be working towards a counterspace capability.

Space Situational Awareness — India 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.[638] In September 2019, ISRO began Project NETRA (Network for space object Tracking and Analysis), which is intended to give India its own SSA network by bringing together radars, telescopes, data processing, and a control center.[639] It will start by focusing on identifying and tracking objects in LEO, but eventually is hoped to have the ability to detect objects in GEO. ISRO announced in December 2020 that its SSA Control Centre in Bengaluru is now operational, stating that "the Directorate of SSA and Management (DSSAM) has been established to engage in evolving improved operational mechanisms to protect space assets through effective coordination amongst ISRO centres, other space agencies and international bodies, and establishment of necessary supporting infrastructure."[640] There have also been talks about possibly signing a space situational awareness agreement with the United States, but that has not yet been completed.

Counterspace Policy, Doctrine, and Organization — India does not currently 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.

There was a draft Geospatial Information Regulation Bill in 2016, but it did not progress; in February 2021, the Indian government announced that it was deregulating geospatial information.[641]

633 "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.

634 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.

635 Ibid.

636 Rajeswari Pillai Rajagopalan, "What Are India's Plans for Directed Energy Weapons?" The Diplomat, Sept. 24, 2020, https://thediplomat.com/2020/09/what-are-indias-plans-for-directed-energy-weapons/?fbclid=IwAR3dz8nWstygBBnOIHJoSO8EYMMbwPFwQwSmRPNYhsqKJJxgajNWSCHvdzM

637 Rajat Pandat, "DRDO plans Star Wars-style weapons for battles of future," Times of India, Sept. 14, 2020, https://timesofindia.indiatimes.com/india/drdo-plans-star-wars-style-weapons-for-battles-of-future/articleshow/78096712.cms

638 "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.

639 Madhumathi D.S., "ISRO initiates 'Project NETRA' to safeguard Indian space assets from debris and other harm," The Hindu, September 24, 2019, https://www.thehindu.com/sci-tech/science/isro-initiates-project-netra-to-safeguard-indian-space-assets-from-debris-and-other-harm/article29497795.ece.

640 Chethan Kumar, "Isro's inaugurates space object tracking centre," Times of India, Dec. 16, 2020, http://timesofindia.indiatimes.com/articleshow/79755718.cms.

641 Anusuya Datta, "India's Decision To De-Regulate Geospatial Information Is Significant In So Many Ways," Geospatial World, February 22, 2021, https://www.geospatialworld.net/blogs/indias-decision-to-de-regulate-geospatial-information-is-significant-in-so-many-ways/.

In October 2007, the Defence Space Vision was released, and listed intelligence, surveillance, reconnaissance, communication, and navigation as primary thrust areas.[642] In 2010, the Ministry of Defence 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." [643]

In June 2010, India established an Integrated Space Cell, located in the Integrated Defence Headquarters, which is comprised of all three branches of India's armed forces.[644] The Integrated Space Cell was in charge of defense-specific space capability requirements and was 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."[645] There has been talk by the Ministry of Home Affairs of a "Border Space Command," that would use space capabilities to monitor India's disputed borders.[646] 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." [647]

In April 2019, India started a Defence Space Agency (DSA) that would coordinate the space assets of the three branches of the Indian armed forces and work on space protection policies for Indian space assets.[648] It will eventually have 200 personnel assigned to it and will incorporate the Defence Satellite Control Centre and the Defence Imagery Processing and Analysis Centre.[649] It was followed by the establishment in June 2019 of the Defence Space Research Organisation, which would conduct research and provide technical support to the DSA.[650] With these new organizations, it is possible that India is shifting to a more offensive approach to its counterspace capabilities, but it is too soon to be certain. The fact that India reportedly held a tabletop exercise (IndSpaceEx) to game out space warfare possibilities and identify gaps/weaknesses in its space security in July 2019 does indicate a willingness to at least theoretically consider using these capabilities.[651] Statements by G Satheesh Reddy, head of DRDO, in April 2019 that "We are working on a number of technologies like DEWs, lasers, electromagnetic pulse (EMP) and co-orbital weapons etc. I can't divulge the details, but we are taking them forward," do lend credence to the idea that India is considering many different options.[652]

POTENTIAL MILITARY UTILITY

India reportedly earned Rs 1,245 crore ($178 million) from 2014-2019 launching foreign satellites; as of November 2020, India had launched 328 foreign satellites.[653] India has been using satellite technologies for strategic purposes: reconnaissance, communications, and navigations. As of January 2021, according to the Union of Concerned Satellites'

642 Rajat Pandit, "Dedicated satellite for Navy by year-end," The Times of India, May 10, 2010.

643 Ibid.

644 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.

645 Sudha Ramachandran, "India goes to war in space," Asia Times, June 18, 2008, http://www.atimes.com/atimes/South_Asia/JF18Df01.html.

646 Rajagopalan, "Need for an Indian Military Space Policy," pp. 206-207.

647 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.

648 Vivek Raghuvanshi, "India to launch a defense-based space research agency," Defense News, June 12, 2019, https://www.defensenews.com/space/2019/06/12/india-to-launch-a-defense-based-space-research-agency/.

649 Ibid.

650 Ibid.

651 Rajeswari Pillai Rajagopalan, "A First: India to Launch First Simulated Space Warfare Exercise: Reports of a tabletop wargame speak to India's ongoing efforts to develop its space policy," The Diplomat, June 12, 2019, https://thediplomat.com/2019/06/a-first-india-to-launch-first-simulated-space-warfare-exercise/.

652 Rajat Pandit, "Satellite killer not one-off, India working on star wars armoury," Times of India, April 7, 2019, https://timesofindia.indiatimes.com/india/satellite-killer-not-a-one-off-india-working-on-star-wars-armoury/articleshow/68758674.cms.

653 T.E.Narasimhan, "Isro revenue from commercial satellite launches up by 40%: Minister," Business Standard, December 13, 2019, https://www.business-standard.com/article/current-affairs/isro-revenue-from-commercial-satellite-launches-up-by-40-minister-119121300298_1.html; "India Set To Touch 328 Foreign Satellite Launches On Saturday," IANS, November 6, 2020, https://economictimes.indiatimes.com/news/science/india-set-to-touch-328-foreign-satellite-launches-on-saturday/articleshow/79076632.cms.

05

Satellite Database, India had 51 active satellites.[654] The first satellite created specifically for the military was the GSAT-7 communications satellite, launched in August 2013.[655] 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.[656] 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.[657] 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.[658]

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 another ASAT, this capability is more likely to be useful as a bargaining chip or a way to demonstrate that India is keeping pace with China.

654 UCS Satellite Database, January 1, 2021, https://www.ucsusa.org/resources/satellite-database.

655 Amit R. Saksena, "India and Space Defense," The Diplomat, March 22, 2014, http://thediplomat.com/2014/03/india-and-space-defense/.

656 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.

657 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.

658 Lele, "India's Strategic Space Programme," p. 191.

06 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 motivation for doing so at this point. Iran's military appears to have an independent ability to launch satellites, separate from the civil space program. Iran has not demonstrated any ability to build homing kinetic kill vehicles, and its ability to build nuclear devices is still fairly constrained. Iran has demonstrated an EW capability 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.[659] However, many other experts discount the ability to use a primitive nuclear device in this way,[660] and state that this is a scare tactic designed to promote missile defense.[661]

Iran is also developing space launch capabilities, both civil and military. 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 theoretically 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 initially meant to have been launched in 2010.[662] Its delay 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.[663] A second test in July 2017 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.[664]

659 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.

660 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.

661 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/.

662 Center for Strategic and International Studies, "Simorgh," Missile Threat, accessed March 21, 2018, https://missilethreat.csis.org/missile/simorgh.

663 Bill Gertz, "Iran Conducts Space Launch," Washington Free Beacon, April 20, 2018, http://freebeacon.com/national-security/iran-conducts-space-launch/.

664 "Iran Announces First Successful Simorgh Test Launch," SpaceFlight101.com, July 29, 2017, http://spaceflight101.com/iran-announces-first-successful-simorgh-test-launch/.

In January 2019, U.S. Secretary of State Mike Pompeo warned Iran about holding what he termed “provocative” space vehicle launches.[665] Iran has experienced a string of space launch failures. Iran held a Simorgh launch in January 2019 which failed to launch its satellite, Payem.[666] Intelligence analysts believe that Iran attempted and failed in the launch of another satellite in February 2019, the Doosti satellite, using a Safir rocket.[667] In August 2019, commercial satellite imagery from Planet documented a launch pad explosion of an Iranian rocket at the Imam Khomeini Space Center.[668] The type of launch pad where the explosion took place was the same kind used to launch Safir rockets. In February 2020, Iran tried to launch the Zafar I, a communications satellite, via the Simorgh SLV; however, it experienced an anomaly at some point between the second and third stages. Ahmad Hosseini, Defense Ministry space program spokesperson, stated, "Stage-1 and stage-2 motors of the carrier functioned properly and the satellite was successfully detached from its carrier, but at the end of its path it did not reach the required speed for being put in the orbit."[669]

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 less than ideal as counterspace launch vehicles.[670] Satellite imagery has detected a limited number of what appear to be engine tests at the Islamic Revolutionary Guard Corps (IRGC)’s Jihad Self-Sufficiency Organization at the Shahroud facility, and in February 2020, Iranian officials released imagery of a motor being tested there, which they stated was of the Salman engine (intended to be a smaller upper stage motor).[671] Footage showed that the developers appear to have been able to make at least two technologies that would be helpful for an SLV program and also a long-range ballistic missile capability: carbon fiber motor casings and thrust vector control (via flexible nozzles).[672] The same day that the Salman motor footage was released, Iranian news reported that a solid-fuelled SLV, the Zuljanah, was finished and would able to launch the Nahid I satellite, potentially as early as June 2020.[673]

In April 2020, the IRGC launched from its Shahroud base a satellite (Noor-1) on a previously unknown SLV, the Qassed.[674] This SLV used a combination of liquid and solid fuel based respectively on the Iranian Ghadr-110 medium range ballistic missile and Salman solid-fueled rocket engine, has three stages, and can be launched via a TEL. Noor-1 was described as a military reconnaissance satellite which appears to be a 6U cubesat; it was detected in a SSO at an altitude of 425 km.[675] The IRGC also announced in April 2020 the existence of its Aerospace Force’s Space Command after the launch by the Qassed SLV.[676] Ali Jafarabadi, head of IRGC’s space force, announced in a June 2020 with Tasnim News that Iran is working on an all solid-fuel Qassed-2 SLV, which he said is lighter and can carry payloads farther, and indicated an interest in launching something to GEO.[677]

665 “U.S. Warns Iran Against 'Provocative' Space Vehicle Launches,” RFE-RL, January 4, 2019, https://www.rferl.org/a/us-warns-iran-space-vehicle-launch-missile-ballistic-nuclear/29690741.html.

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

667 Jon Gambrell, “Images Suggest Iran Has Attempted a Second Satellite Launch,” Times of Israel, February 7, 2019, https://www.timesofisrael.com/images-suggest-iran-launched-satellite-despite-us-criticism/; https://www.space.com/43260-iran-second-satellite-launch-possible-failure.html.

668 Geoff Brumfiel, “Iranian Rocket Launch Ends In Failure, Imagery Shows,” NPR, August 29, 2019, https://www.npr.org/2019/08/29/755406765/iranian-rocket-launch-ends-in-failure-images-show

669 Mike Wall, “Iran satellite launch fails to reach orbit,” Space.com, February 10, 2020, https://www.space.com/iran-satellite-launch-failure-zafar-1.html

670 Fabian Hinz, “Iran’s Solid-Propellant SLV Program is Alive and Kicking,” ArmsControlWonk.com, February 14, 2020, https://www.armscontrolwonk.com/archive/1208906/irans-solid-propellant-slv-program-is-alive-and-kicking/

671 Hinz, ibid.

672 Hinz, ibid.

673 Hinz, ibid.

674 “Iran’s Military Satellite Launch Full Of Surprises,” SpaceWatchGlobal, April 2020, https://spacewatch.global/2020/04/irans-military-satellite-launch-full-of-surprises/.

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

676 Ibid.

677 Khosro Kalbasi, June 8, 2020, https://twitter.com/KhosroKalbasi/status/1269971351475011584.

678 Center for Security and International Studies, "Iran's Ballistic Missiles," Missile Threat, accessed March 21, 2018, https://missilethreat.csis.org/country/iran/.

679 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.

680 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.

681 David Wright, "Another Iranian Satellite Launch: Navid," All Things Nuclear, February 6, 2012, https://allthingsnuclear.org/dwright/another-iranian-satellite-launch-navid.

682 "Iran's Safir Rocket Successfully Launches Fajr Satellite Into Orbit," SpaceFlight101.com, February 2, 2015, https://spaceflightnow.com/2015/02/02/iranian-satellite-successfully-placed-in-orbit/

683 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.

684 "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/; "Iran Completes Construction Of Nahid-2 Satellite," Mehr News Agency, January 21, 2021, https://en.mehrnews.com/news/168843/Iran-completes-construction-of-Nahid-2-satellite.

FIGURE 16 - IRANIAN BALLISTIC MISSILES

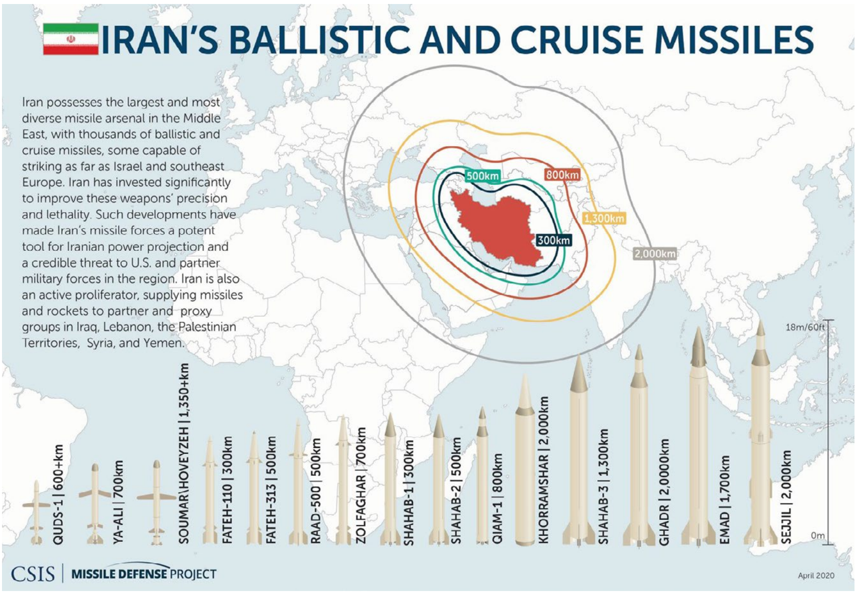


Image Credit: CSIS[678]

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 primarily 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 five satellites into orbit: Omid (2009),[679] Rasad (2011),[680] Navid (2012),[681] Fajr (2015)[682] and Noor-1 (2020).

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,[683] both domestically-developed and through bilateral cooperation with other countries, but many of those plans have been significantly delayed. Iran first announced that it would attempt to launch its Nahid-2 communications satellite before the end of 2018; at writing (February 2021), its construction is complete and it is intended to be sent to the Iranian Space Agency by the end of March 2021 for a launch in the coming year.[684]

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 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.[685] 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.[686]

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.[687] The United States confirmed that a UAV had landed in Iran and asked for its return.[688] 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.[689] While the ability to conduct such a spoofing attack on the civil GPS signal has been demonstrated,[690] conducting a similar attack on the military GPS signal would be much more challenging because it is encrypted. It is possible that Iran may

685 "Satellite Jamming in Iran: A War Over Airwaves," Small Media Lab, November 2012, https://smallmedia.org.uk/media/projects/files/satjam.pdf

686 Peter B. de Selding, "ITU Implores Iran to Help Stop Jamming," SpaceNews, March 26, 2010, https://spacenews.com/itu-implores-iran-help-stop-jamming/.

687 Greg Jaffe and Thomas Erdbrink, "Iran Says It Downed U.S. Stealth Drone; Pentagon Acknowledges Aircraft Downing," 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.

688 Rick Gladstone, "Iran is Asked to Return U.S. Drone," 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.

689 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/.

690 "Spoofing a Superyacht At Sea," UT News, July 30, 2013, https://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea/.

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.[691]

In August 2019, the U.S. government issued public warnings to commercial shipping about potential Iranian jamming and spoofing of space services.[692] The warning cites several incidents of ships reporting GPS interference, bridge-to-bridge communications spoofing, and/or other communications jamming.[693] Unnamed U.S. officials told CNN that Iran had placed GPS jammers on Iran-controlled Abu Musa Island near the entrance to the Strait of Hormuz, but so far they have only affected civilian GPS signals and not U.S. military ships and aircraft.

There were reports in March 2020 of "circle spoofing" of GPS devices around the staff college for Iran's Army, the AJA University of Command and Staff.[694] There was another incident of circle spoofing detected by the fitness app Strava around an Iranian government facility in Tehran.[695]

Space Situational Awareness — Iran is developing limited SSA capabilities that could be used to track and target future counterspace capabilities, but currently appear to be very limited in capability and coverage. In 2013, a center in Delijan was opened that was intended to provide Iran with space object monitoring capabilities via electro-optical, radar, and radio methods.[696] In 2018, Brigadier General Hossein Salami, the deputy commander of Iran's Islamic Revolutionary Guard Corps, said that Iran had the ability to monitor satellites in LEO.[697]

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 and miniaturize it, develop a ballistic missile or SLV that can carry it, and mate the two, it would theoretically be 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.[698]

691 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/.

692 Ryan Browne and Barbara Starr, "U.S. Government Warns of Iranian Threats to Commercial Shipping, Including GPS Interference," CNN, August 7, 2019, https://www.cnn.com/2019/08/07/politics/us-warns-of-iranian-threats-to-shipping/.

693 Maritime Administration, "Persian Gulf, Strait of Hormuz, Gulf of Oman, Arabian Sea, Red Sea-Threats to Commercial Vessels by Iran and its Proxies." U.S. Department of Transportation, MSCI Advisory 2019-012, August 7, 2019, https://www.maritime.dot.gov/content/2019-012-persian-gulf-strait-hormuz-gulf-oman-arabian-sea-red-sea-threats-commercial-vessels

694 Dana Goward, "GPS Circle Spoofing Discovered In Iran," GPS World, April 21, 2020, https://www.gpsworld.com/gps-circle-spoofing-discovered-in-iran/

695 Ibid.

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

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

698 "Collateral Damage to Satellites from an EMP Attack," Defense Threat Reduction Agency, August 2010, https://apps.dtic.mil/dtic/tr/fulltext/u2/a531197.pdf.

07 Japan

ASSESSMENT

Japan has long been a well-established space actor and its space activities have historically been entirely non-military in nature. In 2008, Japan released a Basic Space Law that allowed for national security-related activities in space and since then, government officials have begun to publicly speak about developing various counterspace capabilities or developing military SSA capacity. Japan is currently undergoing a major reorganization of its military space activities and development of enhanced SSA capabilities to support military and civil applications. While Japan does not have any acknowledged offensive counterspace capabilities, it is actively exploring whether to develop them. Japan does have a latent ASAT capability via its missile defense system but has never tested it in that capacity.

SPECIFICS

DA-ASAT Technologies — Japan has no designated DA-ASAT systems under development or in operation. However, it does have the Standard Missile (SM)-3 sea-based ballistic missile defense interceptor, which the United States demonstrated in 2008 could be used to intercept a satellite with only a software modification (See U.S. Direct-Ascent ASAT; section 3.2). A similar software modification might enable Japan to have a DA-ASAT capability against satellites 600 km or lower, although Japan has never tested the SM-3 in that capacity nor expressed a desire to develop it.[699] Japan is also working with the United States on the 3rd stage rocket motor and nose cone of the SM-3 Block 2A interceptor, which is intended to be a more capable hit-to-kill missile interceptor. The SM-3 Block 2A has a faster burn-out speed than its earlier iteration and thus could theoretically reach any satellite in LEO if used in a DA-ASAT role.[700] It successfully intercepted a threat-representative ICBM target during a flight test in November 2020.[701]

Co-Orbital Technologies — In August 2019, the Japanese government announced that it was deliberating whether to develop a satellite that could be used to intercept foreign threat satellites.[702] The goal would be to make a decision in the coming fiscal year so that if Japan decided to go ahead with such a capability, it could be launched by the mid-2020's. According to a senior Ministry of Defense official, this is because Japan's Self-Defense Forces (SDF) "don't have any defense capability for the satellites."[703] To develop this counterspace capability, the Japanese government reportedly will also research different ways in which to interfere with threat satellites, including cyber attacks, RFI, and robotic arms.[704] It is not known whether this future counterspace capability will be defensive or offensive.

699 Laura Grego, "The AntiSatellite Capability of the Phased Adaptive Approach Missile Defense," Federation of American Scientists Public Interest Report, Winter 2011, p. 3, https://fas.org/pubs/pir/2011winter/2011Winter-Anti-Satellite.pdf.

700 Grego, ibid.

701 Ronald O'Rourke, Navy Aegis Ballistic Missile Defense (BMD) Program: Background and Issues for Congress Updated, Congressional Research Service Report RL33745, December 17, 2019, p. 3, https://fas.org/sgp/crs/weapons/RL33745.pdf; "U.S. Successfully Conducts SM-3 Block IIA Intercept Test Against an Intercontinental Ballistic Missile Target," US DoD Press Release, November 17, 2020, https://www.defense.gov/Newsroom/Releases/Release/Article/2417334/us-successfully-conducts-sm-3-block-iia-intercept-test-against-an-intercontinen/.

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

703 Ibid.

704 Daniel Darling, "Japanese Government Considers Launching a Satellite Interceptor," Defense and Security Monitor, August 26, 2019, https://dsm.forecastinternational.com/wordpress/2019/08/26/japanese-government-considers-launching-a-satellite-interceptor/.

Electronic Warfare — The Japanese government has considered developing jamming capabilities that could be used against both airborne warning and control system (AWACS) planes (possibly by the mid-2020's) and then foreign satellites.[705] In August 2019, the Japanese MoD released a budget request for FY2020 that included a request for a 4.0-billion yen ($38-million) program for a "study on electromagnetic disruption system" and purchasing equipment that could detect when its satellites are being electromagnetically interfered with.[706]

Space Situational Awareness — The Japan Aerospace Exploration Agency (JAXA) has been the primary source of Japan's SSA capabilities until recently. JAXA's Kamisaibara Space Guard Center has a radar facility that can see up to 10 objects of a diameter of 1 meter or great to an altitude of 2000 km, and the Bisei Space Guard Center has an optical telescope for SSA tracking to GEO.[707] Japan is also developing an SSA analysis system at Tsukuba Space Center. By FY 2023, JAXA plans to have a new telescope in place in the Bisei Space Guard Center that can detect objects 10 cm in diameter out to 650 km.[708]

In 2019, the United States and Japan announced they were planning to connect their SSA data starting in FY 2023.[709] Japan's SDF does not have its own SSA capabilities but has been working on developing them via U.S. technical assistance since FY 2018. The SDF hopes to be able to monitor GEO and is supposed to have the SSA system that could do it be completed by FY 2022.[710] The Japanese MoD intends for its future SSA network to be composed of both ground- and space-based elements. The SDF SSA system is intended to be tied to the U.S. SSA network, and both hope to be linked to JAXA's network. The fact sheet for the April 2019 2+2 Dialogue held between U.S. and Japanese officials mentioned the possibility of putting U.S. SSA sensors on Japan's Quasi Zenith Satellite System (QZSS) GPS augmentation constellation.[711] The USAF's 2021 budget documents included a request for funding two U.S. SSA payloads on the QZSS that would improve "Geostationary Earth Orbit (GEO) Space Situational Awareness capabilities over the Eurasian theater and facilitates resilient capabilities in the Space Surveillance Network (SSN)."[712]

Counterspace Policy, Doctrine, and Organization — Japan historically defined peaceful uses of outer space to be non-military, a definition that was made official by a 1969 Diet resolution. However, in 2008, the Japanese Diet passed the Basic Space law that allowed space to be used for national security purposes as long as it would be defensive in nature.[713] This was part of a larger shift to thinking about incorporating space into national security needs. The Cabinet office created two organizations within to help focus on the foundations for space security policy: what is now the National Space Policy Secretariat in July 2012, and the Strategic Headquarters for Space Development in 2015.[714] The 2018 National Defense Program Guidelines stated, "To ensure superiority in use of space at all stages from peacetime to armed contingencies, SDF will also work to strengthen capabilities including mission assurance capability and capability to disrupt opponent's

705 "Satellite interceptor sought by mid-2020s," ibid.

706 "Japan requests record $50 billion defense budget in eighth straight increase," The Defense Post, August 30, 2019, https://thedefensepost.com/2019/08/30/japan-record-defense-budget-50-billion.

707 Doug Messier, "Preventing Collisions Between Debris and Spacecraft," Parabolic Arc, May 9, 2017, http://www.parabolicarc.com/2017/05/09/preventing-collisions-between-debris-spacecraft/#more-61468

708 "Japan, US to collaborate on space surveillance," The Mainichi Japan, March 30, 2019, https://mainichi.jp/english/articles/20190330/p2a/00m/0na/002000c.

709 Ibid

710 Ibid

711 Joint Statement of the Security Consultative Committee, April 19, 2019, p. 3, https://www.mofa.go.jp/files/000470738.pdf.

712 Theresa Hitchens, "Air Force Funds Hosted Payloads On Japan Sats," Breaking Defense, February 19, 2020, https://breakingdefense.com/2020/02/air-force-funds-hosted-payloads-on-japan-sats/.

713 Basic Space Law (Law No.43 of 2008), May 21, 2008, https://stage.tksc.jaxa.jp/spacelaw/country/japan/27A-1.E.pdf , p. 2

714 Ryo Hinata-Yamaguchi, "One Small Step for Japan's Space Security Strategy," East Asia Forum, April 1, 2020, https://www.eastasiaforum.org/2020/04/01/one-small-step-for-japans-space-security-strategy/

command, control, communications and information."[715] The guidelines also discussed how for space and cyber, "establishing international rules and norms has been a security agenda."[716] The guidelines directed Japan to build a "Multi-Domain Defense Force," as its defense capability which would bring together "capabilities in all domains including space, cyberspace and electromagnetic spectrum; and is capable of sustained conduct of flexible and strategic activities during all phases from peacetime to armed contingencies."[717] The SDF would, in cases of armed attack against Japan, be permitted to "block and eliminate the attack by leveraging capabilities in space, cyber and electromagnetic domains."[718]

In June 2020, Japan released its "Outline of the Basic Plan on Space Policy." This document identifies "ensuring space security" as one of the Basic Space Plan's goals and focuses on satellites for positioning and maritime domain awareness, cooperation with allies on SSA sharing, becoming involved in international discussions on rules, and focusing on mission assurance.[719]

Japan has also announced steps to reorganize its military space activities. In January 2020, during remarks at the 60th anniversary of the Treaty of Mutual Cooperation and Security Between the United States and Japan, Prime Minister Shinzo Abe noted the need to make the U.S.-Japan alliance more "robust" and "to make it a pillar for safeguarding peace and security in both outer space and cyberspace."[720] Abe also announced at a session of the Diet in January 2020 that Japan will "drastically bolster capability and systems in order to secure superiority."[721] During that speech, he announced that Japan would be establishing its Space Domain Mission Unit (SDMU) in April 2020, with the goal of having it be fully operational by 2022.[722] It was indeed stood up in May 2020 with 20 personnel but is now expected to reach full operations in FY 2023.[723] The SDMU is expected to grow to 100 personnel, and will carry out SSA to protect Japanese satellites. The SDMU will be part of Japan's Air Self-Defense Force and is intended to work with both USSPACECOM and JAXA.

POTENTIAL MILITARY UTILITY

Japan currently possess very limited potential counterspace capabilities. Japan could potentially use its limited SSA capabilities to detect, track, and target a modified SM-3 missile as a DA-ASAT against an adversary satellite in LEO, perhaps with additional tracking assistance and intelligence from the United States. Japan likely possesses the technological foundations to conduct EW against space capabilities, but the military utility and effectiveness of its ability to do so is unknown.

715 Japanese Ministry of Defense, National Defense Program Guidelines for FY 2019 and Beyond, December 18, 2018, p. 20, https://www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/20181218_e.pdf.

716 Guidelines, p. 4

717 Guidelines, p. 11

718 Guidelines, p. 12

719 Outline of the Basic Plan on Space Policy (Provisional Translation), National Space Policy Secretariat, Cabinet Office, Japan, June 30, 2020, https://www8.cao.go.jp/space/english/basicplan/2020/abstract_0701.pdf, p. 6.

720 "Japan To Stand Up Space Domain Mission Unit In April 2020 To Counter Threats To Satellites," SpaceWatch Global, January 2020, https://spacewatch.global/2020/01/japan-to-stand-up-space-domain-mission-unit-in-april-2020-to-counter-threats-to-satellites/.

721 Mari Yamaguchi, "Abe says new unit will defend Japan from space tech threats," Associated Press, January 20, 2020, https://apnews.com/2d88b7c34a5d004eaa59791b8587579d.

722 "Japan to Stand Up," ibid

723 Yoshitako Ito, "SDF's 1st Outer Space Unit Begins Satellite Mission At Base In Tokyo," Asahi Shimbun, May 18, 2020, http://www.asahi.com/ajw/articles/13383396.

08 North 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.[724]

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.[725]

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 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.[726]

Kim Jong Un announced in the annual 2017 New Year's Address that the country was nearly ready to flight-test an ICBM.[727] There were then two ICBM tests in 2017 of a relatively new system, the Hwasong-14. North

724 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/.

725 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.

726 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/.

727 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.

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 U.S. cities and targets in space above LEO potentially at risk.[728] The Hwasong-14 is a two-stage liquid fuel design.

The Hwasong-15 (KN-22) was launched for the first time on Nov. 29, 2017, when this liquid-fueled ICBM flew on a lofted trajectory to an altitude of 4,500 km.[729] 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."[730] 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."[731]

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.[732]

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.[733] Although operational, the reliability of the Unha-3 is not assured. The TD-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.[734] The Unha-3 was used to put the second satellite (Kwangmyŏngsŏng 4) into orbit in 2016.[735] Commercial imagery in March 2019 of North Korea's Sohae Satellite Launching Station indicated that it may have returned to normal operations.[736]

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.[737]

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

728 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.

729 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/.

730 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.

731 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/.

732 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/.

733 John Schilling, "Where's That North Korean ICBM Everyone Was Talking About?" 38 North, March 12, 2015, https://www.38north.org/2015/03/jschilling031215/.

734 Center for Strategic and International Studies, "Taepodong-2 (Unha-3)," https://missilethreat.csis.org/missile/taepodong-2/.

735 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.

736 Jack Liu, Irv Buck, and Jenny Town, "North Korea's Sohae Satellite Launch Facility: Normal Operations May Have Resumed," 38North.org, March 7, 2019, https://www.38north.org/2019/03/sohae030719/

737 Center for Strategic and International Studies, "Taepodong-2 (Unha-3)," https://missilethreat.csis.org/missile/taepodong-2/.

to match the world-level satellite delivery capability in the field of outer space development."[738] A parade in January 2021 showed off what appears to be a new SLBM.[739]

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.[740] Additionally, it is unknown how large of a yield from a nuclear warhead is necessary to affect the U.S. electrical grid.[741] Although North Korea likely demonstrated a thermonuclear capability in September 2017,[742] 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.[743] 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.

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 suggests the satellite was either not under any stabilization or was not functional after deployment.[744] 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.[745] 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.[746] The 2016 version reportedly weighed almost twice as much as the 2012 satellite, at around 200 kg.[747] The satellites and associated objects are in a normal and predictable orbit and do not pose a significant collision threat to other space objects.

738 "Kim Jong Un Watches Ground Jet Test of Newly Developed High-Thrust Engine," Korean Central News Agency, March 19, 2017, https://kcnawatch.org/newstream/1489876327-610396847/kim-jong-un-watches-ground-jet-test-of-newly-developed-high-thrust-engine/

739 Josh Smith and Sangmi Cha, "North Korea Shows Off New Submarine-Launched Missiles After Rare Party Congress," Reuters, January 14, 2021, https://www.reuters.com/article/us-northkorea-politics/north-korea-shows-off-new-submarine-launched-missiles-after-rare-party-congress-idUSKBN29J2YG.

740 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/.

741 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/.

742 North Korea: Overview, Nuclear Threat Initiative, last updated October 2020, https://www.nti.org/learn/countries/north-korea/.

743 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.

744 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/.

745 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.

746 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.

747 Michael Elleman, "North Korea Launches Another Large Rocket: Consequences and Options," 38 North, February 10, 2016, http://www.38north.org/2016/02/melleman021016.

FIGURE 17 - KWANGMYONGSONG-4

Two views of the purported earth-observation satellite Korea launched in January 2016.
Image credit: chinaspaceflight.com.[748]

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.[749] 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.[750] Any serious attempt at orbital counterspace would require a sophistication that is far beyond the capacity of North Korea for the foreseeable future.

748 “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.

749 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/.

750 TLEs for the Kwangmyŏngsŏng satellites are available from the Space Track web site (https://www.space-track.org/). 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.[751] 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 km.

According to unnamed U.S. officials, this type of jamming would not affect U.S. military members who use the military GPS signals.[752] 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,[753] 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.

Space Situational Awareness — There is little publicly available information about North Korea's SSA capabilities. North Korea does have a General Satellite Control Building, which is its headquarters for its National Aerospace Development Administration (NADA), and the facility from which it tracks and monitors its own satellite launches.[754] Since May 2017, imagery has detected construction on an adjacent facility (which most likely is intended to be a space environment test center and most likely does not have SSA capabilities).[755] North Korea has been reported to have Iranian phased array radars as part of its air defense network; their capabilities are unknown.[756]

Counterspace Policy, Doctrine, and Organization — 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 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.[757] North Korean state media clarified in April 2020 that "The purpose of the republic's space development is to adhere to the interests of the state

751 "North Korea 'jamming GPS signals' near South border," BBC News, April 1, 2016, http://www.bbc.com/news/world-asia-35940542.

752 "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.

753 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/.

754 Joseph S. Bermudez Jr., "NADA General Satellite Control Building," 38North.org, March 22, 2018, https://www.38north.org/2018/03/nada032318/

755 Dave Schmerler, "Revealed: North Korea's under-development space environment test center," NKPro.com, June 25, 2019, https://www.nknews.org/pro/revealed-north-koreas-new-space-environment-test-center/.

756 Dave Majumdar, "If Donald Trump Attacks North Korea: Beware of Kim's Air Defense Systems," National Interest, April 14, 2017, https://nationalinterest.org/blog/the-buzz/if-donald-trump-attacks-north-korea-beware-kims-air-defense-20207.

757 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.

and to use science and technology to solve scientific and technological problems essential to economic construction and people's lives."[758]

POTENTIAL MILITARY UTILITY

North Korea likely possess very limited military counterspace capabilities. Its lack of SSA capabilities, HTK, and RPO capabilities and very limited space launch capabilities very likely limits it to broad area attacks, such as NUDETs in LEO that could damage large numbers of satellites over a long period of time. Such an attack would have very limited military utility in a conflict.

[758] Elizabeth Shim, "North Korea highlights space program in state media," UPI, April 6, 2020, https://www.spacewar.com/reports/North_Korea_highlights_space_program_in_state_media_999.html.

09 Cyber Counterspace Capabilities

ASSESSMENT

Multiple countries 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 attack 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.[759]

Any cyber attack requires four things: access, vulnerability, a malicious payload, and a command-and-control system.[760] Three primary points of access exist for exploitation, attack, and service denial of space

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

[760] 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/.

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.[761] 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.[762] 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.[763]

761 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/default/files/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.

762 Eric Sterner and Jennifer McArdle, "Cyber Threats in the Space Domain," The American Foreign Policy Council, Defense Technology Program Brief, March 31, 2016, https://www.afpc.org/uploads/documents/Defense%20Brief%20Issue%2015.pdf 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-website-prod.s3.amazonaws.com/s3fs-public/110916_Wood.pdf

763 "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/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf http://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/#gref.

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.[764] 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 advantages, are certain to continue to pursue a "full range" of counter-space capabilities.[765] 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.[766]

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.[767]

764 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.

765 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/SASC%202017%20ATA%20SFR%20-%20FINAL.PDF

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

767 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.

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[768] and Russian software packages[769] 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 foreign telecommunications and aerospace infrastructure.[770] There have also been media reports of U.S. intelligence agencies intercepting shipments of commercial equipment to install "implants",[771] and creating backdoors in commercial encryption software.[772] 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.

768 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.

769 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

770 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.

771 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/.

772 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.

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.[773] 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.[774] In October 2007, the Landsat 7 remote sensing satellite experienced twelve minutes of interference. In June 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. Initial reports traced events to the Kongsberg Satellite Services ground station at Svalbard, but they said their systems could not command NASA satellites.[775] General Robert Kehler, then commander of United States Strategic Command, said there was no evidence to attribute the attacks at the time.[776]

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;[777] 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;[778] physical access, through either covert infiltration or social engineering;[779] and network exploitation or attack, using traditional means.[780] 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 (albeit not specifically space-related air gapped networks).[781] In June 2018, cybersecurity firm Symantec reported on a wide-ranging cyber espionage campaign by a group named Thrip, likely based in China, that included attacks against defense and space-related companies. According to Symantec, Thrip targeted computers at a commercial operator running software that monitors and controls communications satellites.[782]

773 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.

774 "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.

775 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.

776 Ibid.

777 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/.

778 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/.

779 Ibid.

780 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.

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

782 Security Response Attack Investigation Team, "Thrip: Espionage group hits satellite, telcoms, and defense companies," Symantec, June 19, 2018, https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets.

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.[783] In 2011, attackers gained full access to 18 servers supporting multiple mission at the Jet Propulsion Laboratory and stole 87 gigabytes of data.[784] In late 2014, attackers breached NOAA's computer network, including systems used to manage and disseminate satellite weather data and products for the National Environmental Satellite, Data, and Information Service (NESDIS) and the National Earth System Prediction Capability (ESPC).[785] Although the attack itself did not disrupt satellite data, NOAA stopped providing satellite images to the National Weather Service and public-facing services were taken offline for two days while 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."[786] The Symantec report on Thrip also claimed that the group attacked computers running Geographic Information System (GIS) software used for tasks such as developing custom geospatial applications or integrating location-based data into other applications and software for processing satellite imagery.[787]

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 U.S. university students developed a technique for attacking the software in common commercial GPS receivers.[788] 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.[789]

783 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/docs/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.

784 NASA Office of the Inspector General, "Cybersecurity Management and Oversight at the Jet Propulsion Laboratory," National Aeronautics and Space Administration, Report No. IG-19-022, June 18, 2019, https://oig.nasa.gov/docs/IG-19-022.pdf

785 Mary Pat Flaherty, Jason Samenow, and Lisa Rein, "Chinese Hack U.S. Weather Systems, Satellite Network," Washington Post, November 12, 2014, https://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html?utm_term=.d01b2f4051a7.

786 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.

787 Security Response Attack Investigation Team, "Thrip: Espionage group hits satellite, telcoms, and defense companies," Symantec, June 19, 2018, https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets.

788 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.

789 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.

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".[790] 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.[791] 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 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.[792] 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.[793]

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."[794] 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.[795] 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."[796]

In August 2020, a presentation at the Blackhat USA 2020 conference outlined multiple examples of insecure internet communications travelling over satellite links.[797] A researcher built an inexpensive setup that allows him to eavesdrop on Ku band signals from 18 geostationary communications satellites covering the Atlantic Ocean, South America, Europe, and Africa. The captured data included numerous examples of sensitive data, such as aircraft navigational information, system administrator credentials for computer networks, and personal identifying data. The researcher also showed how an attacker can take advantage of the high latency of satellite internet links to hijack a connection.

790 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.

791 Ibid.

792 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/.

793 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.

794 CrowdStrike Intelligence Report: Putter Panda," CrowdStrike, June 9, 2014, https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf.

795 Ibid.

796 Ibid.

797 Dan Goodin, "Insecure satellite Internet is threatening ship and plane safety," Arstechnica.com, August 5, 2020, https://arstechnica.com/information-technology/2020/08/insecure-satellite-internet-is-threatening-ship-and-plane-safety/.

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.[798] Turla's technique, which couples a compromised PC using satellite-based Internet with a MITM attack, hijacks the IP addresses of legitimate users. American and British officials have stated that the Turla group also attempted to masquerade as Iranian hackers to mislead investigators.[799] This approach allows the hacker to anonymize Internet connections, impersonate legitimate high-speed Internet users, spoof DNS requests, and gain access to private networks.[800] 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.[801] Perhaps worst of all, information on these techniques is readily available in the public domain, and the steps are easily replicable by 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.[802] 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.[803] 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.[804]

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.[805] 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.[806] 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.[807]

798 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/.

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

800 Ibid.

801 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/.

802 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.

803 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/.

804 Ibid.

805 David Livingstone and Patricia Lewis, "Space, the Final Frontier for Cybersecurity?", Chatham House, September 2016, https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf

806 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, https://www.semanticscholar.org/paper/Satellite-hacking%3A-A-guide-for-the-perplexed-Fritz/b7ba156257c4a3fef16183a4f153a46af821ee7b

807 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/.

Most notably, this campaign included the physical incapacitation of Ukrainian power grids.[808] 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 achieved would have allowed the attackers to inflict extensive physical damage and bring the power stations permanently offline had they wished to do so.[809]

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.[810] 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.[811] 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.[812] 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.[813] 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 Department.[814] 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.[815] 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

808 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/.

809 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.

810 "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.

811 "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.

812 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.

813 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.

814 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.

815 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.

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.[816] 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, 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.[817] 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;[818] hacks of U.S. 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;[819] 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;[820] and frequent and sustained cyber-espionage and cyber crime campaigns targeted at, among other things, large banks and financial institutions,[821]

816 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.

817 David Sanger, David Kirkpatrick, and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More," New York Times, October 15, 2017, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html.

818 Ibid.

819 Ibid. It is worth noting that these operations are in no way one-sided: there is substantial evidence of similar operations by both the U.S. and South Korean governments.

820 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,"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.

821 David Sanger, David Kirkpatrick, and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More." 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.

cryptocurrency exchanges,[822] and defense and defense-adjacent companies.[823] 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.

In February 2019, multiple anonymous sources claimed that the United States had an on-going program of offensive cyber attacks aimed at undermining Iran's ballistic missile program.[824] The sources claimed that the program included cyber sabotage of Iran's missiles and rockets and may have led to an increase in recent launch failures. If true, the program would be the first public example of cyber attacks being used to physically damage space capabilities.

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.[825]

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 escalation that such can attend such deliberately opaque approaches, as the difficulty of guaranteeing

822 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.

823 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/.

824 David Sanger and William Broad, "U.S. revives secret program to sabotage Iranian missiles and rockets," New York Times, February 13, 2019, https://www.nytimes.com/2019/02/13/us/politics/iran-missile-launch-failures.html.

825 Eric Sterner and Jennifer McArdle, "Cyber Threats to the Space Domain," The American Foreign Policy Council, March 2016, https://www.afpc.org/uploads/documents/Defense%20Brief%20Issue%2015.pdf

a reliable and proportional response can create structural incentives for each side to move first in the event of an impending crisis.[826] 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.[827] 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 point 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.[828] 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 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.[829]

826 Todd Harrison et al, "Escalation and Deterrence in the Second Space Age," Center for Security and International Studies, October 2017, https://www.csis.org/analysis/escalation-and-deterrence-second-space-age

827 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.

828 "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's%20Advanced%20Weapons.pdf

829 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/research/china-dream-space-dream-chinas-progress-space-technologies-and-implications-united-states
"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's%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.

10 **Appendix 01 –** Historical Anti-Satellite Tests in Space by Country

This appendix lists known or suspected anti-satellite (ASAT) tests in space by country. It provides known information about each test, including the date it was conducted, launch site, launch vehicle, interceptor, and target (if known). It also provides a short summary of the outcome of the test and whether it generated any orbital debris.

↗

Note that there may be different definitions for "success." In some cases, the goal of the test was to have an actual intercept of another space object, but in other cases, the objective of the test was to track a specific star or pass within a specific distance of another space object without an actual collision or detonation of the warhead of kill vehicle.

TABLE 12 - HISTORICAL CHINESE ASAT TESTS IN SPACE

DATE	ASAT SYSTEM	ASAT TYPE	LAUNCH SITE	TARGET	NOTES
July 07, 2005	SC-19	Direct Ascent	Xichang	None known	Likely near-miss of orbital target
Feb. 6, 2006	SC-19	Direct Ascent	Xichang	Unknown satellite	Likely near-miss of orbital target
Jan. 11, 2007	SC-19	Direct Ascent	Xichang	FY-1C satellite	Destruction of orbital target
Jan. 11, 2010	SC-19	Direct Ascent	Korla	CSS-X-11 ballistic missile launched from Jiuquan	Destruction of target
Jan. 27, 2013	Possibly SC-19	Direct Ascent	Korla	Unknown ballistic missile launched from Jiuquan	Destruction of target
May 13, 2013	Possibly DN-2	Direct Ascent	Xichang	None known	Likely rocket test
July 23, 2014	Possibly DN-2, (possibly SC-19)	Direct Ascent Korla?	(Jiuquan?)	None known	Likely near-miss of orbital target
Oct. 30, 2015	Possibly DN-3	Direct Ascent	Korla	None known, possible ballistic missile	Likely rocket test
July 23, 2017	DN-3	Direct Ascent	Jiuquan?	Likely ballistic missile	Likely intercept test
Feb. 5, 2018	DN-3	Direct Ascent	Korla	CSS-5 ballistic missile	Likely intercept test

TABLE 13 - HISTORICAL RUSSIAN ASAT TESTS IN SPACE

DATE	ASAT SYSTEM	ASAT TYPE	LAUNCH SITE	TARGET	NOTES
Nov. 1, 1963	IS	Co-orbital	Baikonur	None	Engine and maneuvering test
Apr. 12, 1964	IS	Co-orbital	Baikonur	None	Engine and maneuvering test
Oct. 27, 1967	IS	Co-orbital	Baikonur	None	First launch of KKV
Oct. 20, 1968	IS	Co-orbital	Baikonur	Cosmos 248	Two successful intercepts, debris created
Oct. 23, 1970	IS	Co-orbital	Baikonur	Cosmos 373	Two successful intercepts, debris created
Feb. 25, 1971	IS	Co-orbital	Baikonur	Cosmos 394	Intercept, debris created
Mar. 18, 1971	IS	Co-orbital	Baikonur	Cosmos 400	No intercept, different approach of target
Dec. 3, 1971	IS	Co-orbital	Baikonur	Cosmos 459	Successful intercept, debris created
Feb. 16, 1976	IS	Co-orbital	Baikonur	Cosmos 803	Two successful intercepts, debris created
July 9, 1976	IS	Co-orbital	Baikonur	Cosmos 839	Potential intercept, no debris created
Dec. 17, 1976	IS	Co-orbital	Baikonur	Cosmos 880	Successful intercept, debris created

TABLE 14 - HISTORICAL RUSSIAN ASAT TESTS IN SPACE CONT'D

DATE	ASAT SYSTEM	ASAT TYPE	LAUNCH SITE	TARGET	NOTES
May 23, 1977	IS	Co-orbital	Baikonur	Cosmos 909	Two unsuccessful intercepts, no debris created
Oct. 26, 1977	IS	Co-orbital	Baikonur	Cosmos 959	Successful intercept, no debris created
Dec. 21, 1977	IS	Co-orbital	Baikonur	Cosmos 967	Unsuccessful intercept
May 19, 1978	IS	Co-orbital	Baikonur	Cosmos 970	Successful intercept, debris created
Apr. 18, 1980	IS	Co-orbital	Baikonur	Cosmos 1171	Unsuccessful intercept, debris created
Feb. 2, 1981	IS	Co-orbital	Baikonur	Cosmos 1241	Two failed intercepts, no debris created
June 18, 1982	IS	Co-orbital	Baikonur	Cosmos 1375	Successful intercept, debris created
Nov. 20, 1990	Naryad	Co-orbital	Baikonur	None	No intercept
Dec. 20, 1991	Naryad	Co-orbital	Baikonur	None	No intercept
Dec. 26, 1994	Naryad	Co-orbital	Baikonur	Unknown	Potential intercept, debris created
Aug. 12, 2014	Nudol	Direct Ascent	Plesetsk	None	Rocket test (unsuccessful)
Apr. 22, 2015	Nudol	Direct Ascent	Plesetsk	None	Rocket test (unsuccessful)
Nov. 18, 2015	Nudol	Direct Ascent	Plesetsk	None	Rocket test (successful)
May 25, 2016	Nudol	Direct Ascent	Plesetsk	None	Rocket test (successful)
Dec. 16, 2016	Nudol	Direct Ascent	Plesetsk	None	Rocket test (successful)
Oct. 30, 2017	Burevestnik?	Co-orbital	Plesetsk	None	Released subsatellite at relatively high speed
Mar. 26, 2018	Nudol	Direct Ascent	Plesetsk	None	First test from TEL
Dec. 23, 2018	Nudol	Direct Ascent	Plesetsk	None	Potential KKV, no intercept
June 14, 2019	Nudol	Direct Ascent	Plesetsk	None	Potential KKV, no intercept
Apr. 15, 2020	Nudol	Direct Ascent	Plesetsk	None	Potential intercept, debris created
July 15, 2020	Burevestnik?	Co-orbital	Plesetsk	None	Released subsatellite at relatively high speed
Dec. 16, 2020	Nudol	Direct Ascent	Plesetsk	None	Potential KKV, no intercept

TABLE 15 - HISTORICAL U.S. ASAT TESTS IN SPACE

DATE	ASAT SYSTEM	ASAT TYPE	LAUNCH SITE	TARGET	NOTES
Sept. 22, 1959	High Virgo	Direct Ascent	Unknown	None	Unknown results due to loss of telemetry
Oct. 13, 1959	Bold Orion	Direct Ascent	Unknown	Explorer VI	Success (passed within kill radius)
April 1962	HiHo	Direct Ascent	Unknown	None	Failure
June 1962	HiHo	Direct Ascent	Unknown	None	Successful rocket test
Dec. 17, 1962	Nike Zeus	Direct Ascent	WSMR	None	Success (reached designated point in space)
Feb. 15, 1963	Nike Zeus	Direct Ascent	Kwajalein	None	Successful intercept of designated point in space
Mar. 31, 1963	Nike Zeus	Direct Ascent	Kwajalein	None	Unsuccessful attempt to intercept simulated satellite target
Apr. 19, 1963	Nike Zeus	Direct Ascent	Kwajalein	None	Unsuccessful attempt to intercept simulated satellite target
May 24, 1963	Nike Zeus	Direct Ascent	Kwajalein	Agena D	Successful close intercept
Jan. 4, 1964	Nike Zeus	Direct Ascent	Kwajalein	None	Successful intercept of a simulated satellite target
Feb. 14, 1964	Program 437	Direct Ascent	Johnston Island	Transit 2A Rocket Body	Success (passed within kill radius)
Mar. 1, 1964	Program 437	Direct Ascent	Johnston Island	Unknown	Success (primary missile scrubbed, backup missile passed within kill radius)
Apr. 21, 1964	Program 437	Direct Ascent	Johnston Island	Unknown	Success (passed within kill radius)
May 28, 1964	Program 437	Direct Ascent	Johnston Island	Unknown	Failed (missed intercept point)
Nov. 16, 1964	Program 437	Direct Ascent	Johnston Island	Unknown	Successful Combat Test Launch (passed within kill radius)
March 1965	Nike Zeus	Direct Ascent	Kwajalein	None	-
Apr. 5, 1965	Program 437	Direct Ascent	Johnston Island	Transit 2A Rocket Body	Successful Combat Test Launch (passed within kill radius)
June-July 1965	Nike Zeus	Direct Ascent	Kwajalein	None	Four test intercepts, of which three were successful
Jan. 13, 1966	Nike Zeus	Direct Ascent	Kwajalein	None	Successful intercept with simulated target
Mar. 31, 1967	Program 437	Direct Ascent	Johnston Island	Unknown piece of space debris	Successful Combat Evaluation Launch (passed within kill radius)
May 15, 1968	Program 437	Direct Ascent	Johnston Island	Unknown	Successful Combat Evaluation Launch (passed within kill radius)
Nov. 21, 1968	Program 437	Direct Ascent	Johnston Island	Unknown	Successful Combat Evaluation Launch (passed within kill radius)

TABLE 16 - HISTORICAL U.S. ASAT TESTS IN SPACE CONT'D

DATE	ASAT SYSTEM	ASAT TYPE	LAUNCH SITE	TARGET	NOTES
Jan. 21, 1984	ASM-135	Direct Ascent	aircraft	None	ASM-135 missile fired from F-15 fighter, successful missile test
Nov. 13, 1984	ASM-135	Direct Ascent	aircraft	Star	Failed test
Sept. 13, 1985	ASM-135	Direct Ascent	aircraft	Solwind	Successful test, created 285 pieces of trackable orbital debris
Aug. 22, 1986	ASM-135	Direct Ascent	aircraft	Star	Successful test in tracking
Sept. 29, 1986	ASM-135	Direct Ascent	aircraft	Star	Successful test in tracking
Sept. 29, 1986	ASM-135	Direct Ascent	aircraft	Star	Successful test
Feb. 28, 2000	SM-3	Direct Ascent	ship	USA 193	Successful intercept, debris created

TABLE 17 - HISTORICAL INDIAN ASAT TESTS IN SPACE

DATE	ASAT SYSTEM	ASAT TYPE	LAUNCH SITE	TARGET	NOTES
Feb. 12, 2019	PDV-MK II	direct ascent	Abdul Kalam island	Microsat-R	Unsuccessful intercept
Mar. 27, 2019	PDV-MK II	direct ascent	Abdul Kalam island	Microsat-R	Successful intercept, debris generated

11 Appendix 02 – Imagery of Major Counterspace Test Sites and Facilities

LAUNCH COMPLEXES

CHINA →
Jiuquan

SPACE LAUNCH CENTER AND MISSILE TEST COMPLEX

DN-2, DN-3, SC-19

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 01 - JIUQUAN

A launch complex at the Jiuquan Space Launch Center in the Gobi Desert, Inner Mongolia, is used for testing mobile ballistic missiles. The image shows two TEL launch pads which may be used to launch suborbital targets for ASAT testing.

LAUNCH COMPLEXES

CHINA →
Korla West

MISSILE TEST COMPLEX

DN-2, DN-3, SC-19

41.537300 N 86.353317 E
(garrison complex)

- 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 02 - KORLA WEST COMPLEX

The Korla West test complex near the city of Korla in Xinjiang 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.

LAUNCH COMPLEXES

CHINA →
Korla West

MISSILE TEST COMPLEX

DN-2, DN-3, SC-19

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 03 - KORLA WEST LAUNCH PAD

The ASAT launch pad at Korla West employs a relocatable shelter for TEL concealment. The image shows a TEL shelter placed on the launch pad.

LAUNCH COMPLEXES

CHINA →
Taiyuan

SPACE LAUNCH CENTER AND MISSILE TEST COMPLEX

DN-3

38.840519 N 111.604648 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 04 – TAIYUAN SPACE LAUNCH CENTER MOBILE LAUNCH PAD

Taiyuan Space Launch Center in Shanxi Province 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.

LAUNCH COMPLEXES

CHINA →
Xichang

SPACE LAUNCH CENTER AND MISSILE TEST COMPLEX

DN-2, SC-19

28.249140 N 102.022942 E
(northern 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 05 – XICHANG SPACE LAUNCH CENTER NORTH ASAT PAD

Xichang Space Launch Center in Sichuan possesses launch pads at the northwest and southeast end of the facility possibly supporting SC-19 and DN-2 ASAT tests. This image shows the pad to the NW, which has a relocatable shelter and on-going construction.

LAUNCH COMPLEXES

CHINA →
Xichang

SPACE LAUNCH CENTER AND MISSILE TEST COMPLEX

DN-2, SC-19

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 06 – XICHANG SPACE LAUNCH CENTER SOUTH ASAT PAD

This image shows the SE ASAT launch pad at Xichang, which was the likely launch site for the May 13, 2013 ASAT test that went nearly to GEO.

LAUNCH COMPLEXES

RUSSIA →
Kapustin Yar

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—Image Shown)

48.770544 N 46.303367 E
(missile test complex)

MISSILE TEST AND TRAINING COMPLEX

NUDOL

- December 16, 2016 (possible Nudol ASAT test)

FIGURE 07 - KAPUSTIN YAR MOBILE MISSILE LAUNCH SITE

Kapustin Yar, located in Astrakhan Oblast, has long supported Russian ballistic missile and missile defense testing as well as some early space launches. The mobile ICBM training and launch area at Kapustin Yar is a possible location for the December 16, 2016 Nudol ASAT test.

LAUNCH COMPLEXES

RUSSIA →
Plesetsk

MOBILE MISSILE TEST COMPLEX

NUDOL

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 08 – PLESETSK SPACE LAUNCH CENTER MOBILE MISSILE LAUNCH COMPLEX

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.

LAUNCH COMPLEXES

RUSSIA →
Plesetsk

ROCKOT LAUNCH PAD

63.008092 N 41.551308 E
(Site 133)

- Nov. 20, 1990 (potential Naryad-V launch)
- Dec. 20, 1991 (potential Naryad-V launch)
- Dec. 26, 1994 (potential Naryad-V launch)
- Dec. 25, 2013 (launch of Cosmos 2491)
- May 23, 2014 (launch of Cosmos 2499)
- Mar. 31, 2015 (launch of Cosmos 2504)

FIGURE 09 – PLESETSK SPACE LAUNCH CENTER SITE 133

Site 133 at Plesetsk contains the launch pad for the Rockot booster, which was used to launch the suspected Naryad-V co-orbital ASAT test in the early 1990s and also the first set of Russian RPO payloads into LEO in 2013-2015.

LAUNCH COMPLEXES

RUSSIA →
Plesetsk

SOYUZ-2-1B AND SOYUZ-2-1V LAUNCH PADS

62.927217 N 40.449530 E
(Site 43, Pad 3)

62.928801 N 40.456686 E
(Site 43, Pad 4)

- Jun. 23, 2017 (launch of Cosmos 2519)
- Jul. 10, 2019 (launch of Cosmos 2535 and Cosmos 2536)
- Nov. 25, 2019 (launch of Cosmos 2542)

FIGURE 10 – PLESETSK SPACE LAUNCH CENTER SITE 43

Site 43 at Plesetsk contains the launch pad for the Soyuz-2-1v rocket, which was used launch multiple Russian RPO payloads into LEO since 2017, including Cosmos 2519, Cosmos 2535, and Cosmos 2542 that were involved in potential co-orbital ASAT tests.

LAUNCH COMPLEXES

RUSSIA →
Sary Shagan

SAM AND ABM TEST COMPLEX 51T6, 53T6, 53T6M

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 11 - SARY SHAGAN ABM SILOS

Sary Shagan is a long-standing Russian anti-ballistic missile testing facility located in Kazakhstan. Site 35 possesses two silos for conducting tests and training launches of the 53T6 ABM.

LAUNCH COMPLEXES

RUSSIA →
Baikonur

SPACE LAUNCH CENTER AND MISSILE TEST COMPLEX

IS

46.079749 N 62.932500 E
(Site 90, IS launch complex)

• October 27, 1967 (first test launch of IS ASAT)

FIGURE 12 - BAIKONUR

While the Baikonur Cosmodrome in Kazakhstan is most famous as the historical launch site for Russia's human spaceflight program, it has also supported a large number of military launches. Site 90 was operated as a test launch site for the IS co-orbital ASAT program, using the UR-200 and Tsyklon-2A boosters.

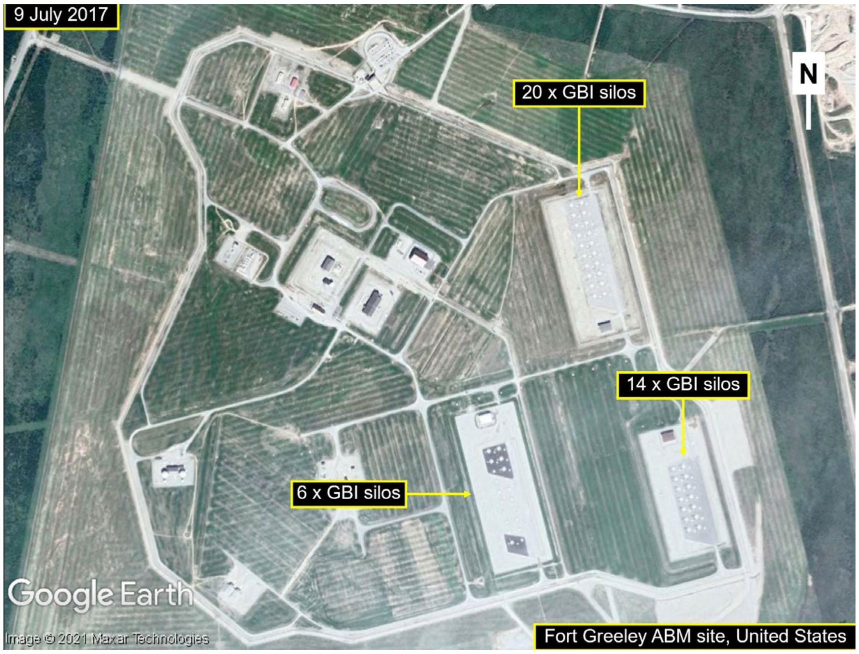
LAUNCH COMPLEXES

ABM COMPLEX GMD

UNITED STATES →
Fort Greely

63.953987 N -145.725365 W

FIGURE 13 - FORT GREELY



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

LAUNCH COMPLEXES

UNITED STATES →
Vandenberg Air Force Base

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—Image Shown)

34.739657 N -120.619205 W
(LC 576-E)

SPACE LAUNCH CENTER AND ABM COMPLEX

FIGURE 14 - VANDENBERG

Vandenberg Air Force Base in California houses various launch facilities used to deliver military payloads into orbit. Shown here is Space Launch Complex 6 (“Slick Six”) that was planned to support the Manned Orbital Laboratory (MOL) and West Coast Space Shuttle launches. Most recently, it has supported Athena and Delta IV launches.

LAUNCH COMPLEXES

UNITED STATES →
Cape Canaveral

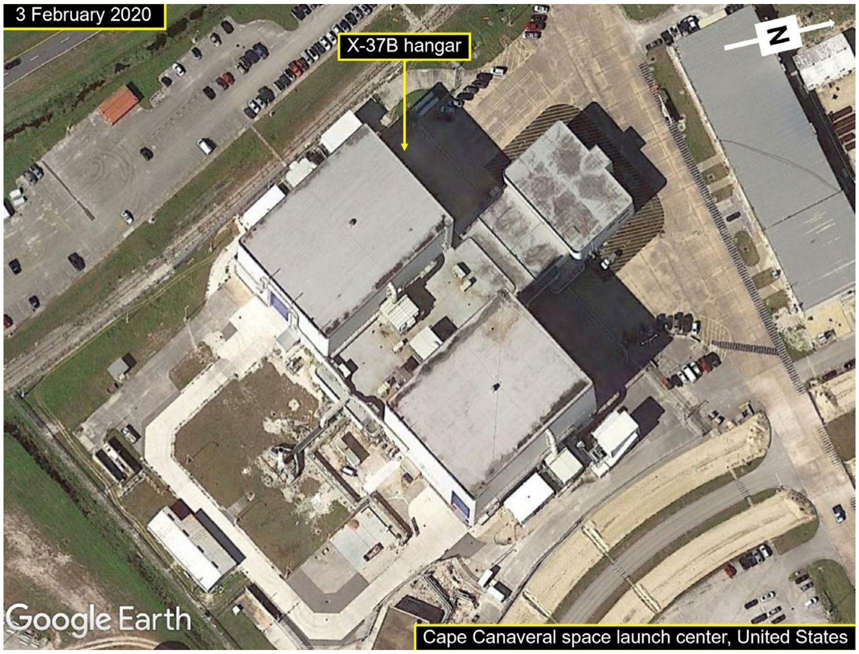
28.583414 N -80.582891 W
(SLC 41)

28.532311 N -80.566601 W
(SLC 37)

28.585802 N -80.654991 W
(X-37B Hangar—Image Shown)

SPACE LAUNCH CENTER X-37B

FIGURE 15 - CAPE CANAVERAL



Cape Canaveral Space Force Station in Florida houses various launch facilities used to deliver military payloads into orbit and is co-located with the Kennedy Space Center, which supports NASA's human spaceflight program. Most recently, Cape Canaveral has become the home of the USSF's X-37B spaceplane. It launches from SLC 41 and began landing at the Kennedy Space Center's Shuttle Landing Facility with OTV-4 in May 2017.

LAUNCH COMPLEXES

INDIA →
Satish Dhawan

SPACE LAUNCH CENTER PSLV

13.733280 N 80.234840 E
(First Launch Pad—Image Shown)

13.719751 N 80.230431 E
(Second Launch Pad)

FIGURE 16 - SATISH DHAWAN

Satish Dhawan Space Centre, located in Sriharikota in Andhra Pradesh, is India's primary space launch center.

LAUNCH COMPLEXES

INDIA →
Abdul Kalam Island

MISSILE TEST COMPLEX AAD, PAD, PDV

20.755135 N 87.088511 E
(Launch Complex IV)

- February 12, 2019 (Unsuccessful DA-ASAT test)
- March 27, 2019 (Successful DA-ASAT test, destroyed Microsat-R)

FIGURE 17 - ABDUL KALAM ISLAND

The Integrated Test Range complex at Abdul Kalam Island (formerly Wheeler Island) is the primary test site for India's antiballistic missile systems. It was also the launch site for both of India's DA-ASAT tests in February and March 2019.

LAUNCH COMPLEXES

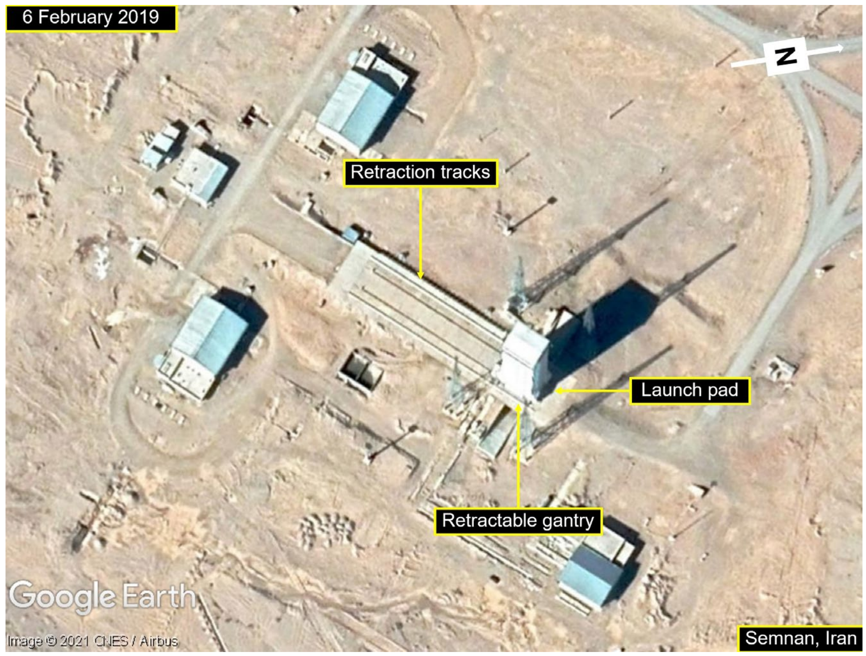
IRAN →
Semnan

35.23472 N 53.92083 E
(Safir Launch Pad—Image Shown)

35.2583 N 53.9547 E
(Imam Khomeini Spaceport)

SPACE LAUNCH CENTER SAFIR, SIMORGH

FIGURE 18 – SEMNAN SPACE CENTER



Semnan Space Center is Iran's primary space launch facility, located 50 kilometers southeast of the city of Semnan in the north of the country. The image shows the Imam Khomeini Spaceport, which is the site for the Simorgh SLV.

LAUNCH COMPLEXES

IRAN →
Shahrud

36.200599 N 055.333928 E

LAUNCH SITE QASSED

FIGURE 19 – SHAHRUD LAUNCH SITE

A third Iranian space launch facility was built approximately 40 kilometers SE of the town of Shahrud in Semnan province. The Shahrud facility appears to be the launch site for Iran's military space launches, the Space Center is Iran's primary space launch facility, located 50 kilometers southeast of the city of Semnan in the north of the country. The image shows the Imam Khomeini Spaceport, which is the site for the Simorgh SLV.

LAUNCH COMPLEXES

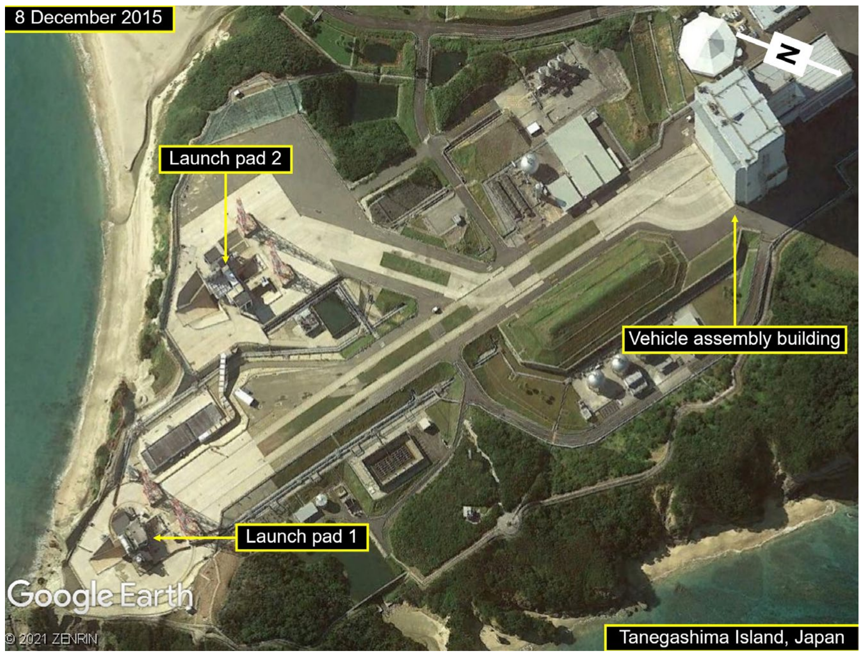
JAPAN →
Tanegashima

30.402291 N 130.974102 E

SPACE CENTER

H-IIA

FIGURE 20 - TANEGASHIMA SPACE CENTER



Tanegashima Space Center is Japan's largest space launch facility and located on the southeast coast of Tanegashima island, just south of Kyushu.

LAUNCH COMPLEXES

NORTH KOREA →
Tonghae

40.85 N 129.666667 E

SATELLITE LAUNCHING GROUND TD-1

FIGURE 21 – TONGHAE SATELLITE LAUNCHING GROUND

Tonghae Satellite Launching Ground, also known as Musudan-ri, is a ballistic missile and space launch site in North Korea.

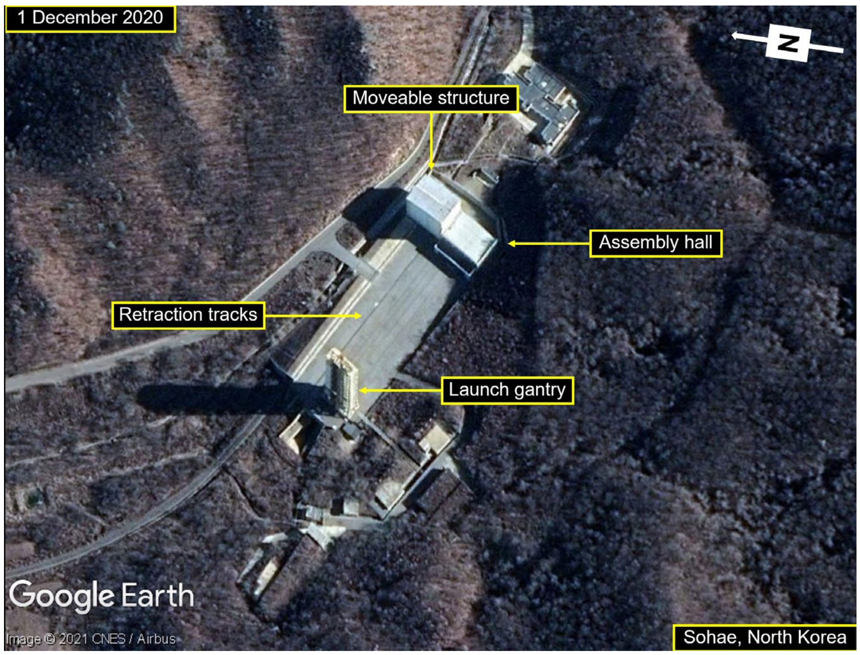
LAUNCH COMPLEXES

NORTH KOREA →
Sohae

39.660 N 124.705 E

SATELLITE LAUNCHING STATION UNHA

FIGURE 22 – SOHAE SATELLITE LAUNCHING STATION



Tonghae Satellite Launching Ground, also known as Tongch'ang-dong Space Launch Center and Pongdong-ri, is a ballistic missile and space launch site in North Korea.

DIRECTED ENERGY WEAPONS COMPLEXES

CHINA →

LASER TEST SITES

31.532158 N 104.740708 E
(Mianyang)

31.901428 N 117.162222 E
(Hefei)

34.7475 N 113.781767 E
(Zhengzhou)

43.790506 N 125.442814 E
(Changchun)

FIGURE 23 – LASER TEST SITE NEAR MIANYANG

China currently has five potential facilities for conducting research and development of high-power directed energy weapons in a counterspace role. The image above shows one suspected facility near Mianyang in Sichuan Province.

DIRECTED ENERGY WEAPONS COMPLEXE

CHINA →

LASER TEST SITES

41.761422 N 87.418331 E
(Bohu)

FIGURE 24 – LASER TEST SITE NEAR BOHU

The above image shows a second suspected laser test site near Bohu, which is close to the Korla West missile test facility that is prominent in Chinese DA-ASAT testing.

DIRECTED ENERGY WEAPONS COMPLEXE

RUSSIA →

MOBILE LASER DEPLOYMENT SITES

PERESVET BASES

56.899222 N 40.578117 E
(Teykovo)

56.573328 N 48.039010 E
(Yoshkar Ola)

58.133634 N 60.522106 E
(Svobodnyy)

55.270300 N 83.017993 E
(Novosibirsk)

53.555585 N 83.825132 E
(Barnaul—Image Shown)

FIGURE 25 – PERESVET DEPLOYMENT SITE NEAR BARNNAUL

Russia has recently deployed its new Peresvet mobile laser dazzler system to five sites, all of which are located near mobile ICBM garrisons. The above image shows the Peresvet shelter near Barnaul in the Altai Krai region, with the Peresvet vehicle itself partially emerging from the building.

SENSOR COMPLEXES

CHINA →

RADAR COMPLEXES

LARGE PHASED-ARRAY RADAR (LPAR) SITES

46.527890 N 130.755269 E
(Huanan)

36.024737 N 118.091972 E
(Yiyuan)

30.286623 N 119.128566 E
(Hangzhou)

41.641212 N 86.236834 E
(Korla—Image Shown)

35.482983 N 106.571819 E
(Kongtong)

FIGURE 26 - LPAR SITE NEAR KORLA

China operates numerous LPARs which provide SSA data and could serve as acquisition sensors for ABM and/or ASAT systems. The image shows the LPAR site near Korla.

SENSOR COMPLEXES

CHINA →

OPTICAL TELESCOPE COMPLEXES

PURPLE MOUNTAIN OBSERVATORY

32.065 N 118.8297 E

FIGURE 27 – PURPLE MOUNTAIN OBSERVATORY

China's main optical SSA capabilities are operated by the Purple Mountain Observatory (PMO), which operates multiple telescopes in seven separate locations that can track satellites throughout all orbital regimes.

60.275210 N 30.545593 E
(77Ya6M)

51.273673 N 58.959036 E
(77Ya6M—Image Shown)

58.506337 N 92.045261 E
(77Ya6DM)

53.139759 N 83.680803 E
(77Ya6DM)

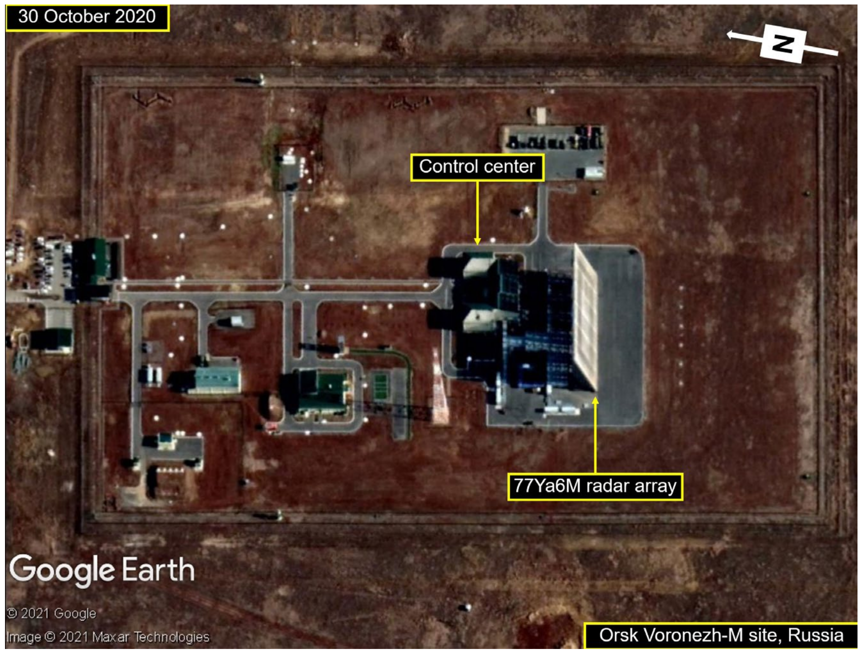
54.857482 N 20.182510 E
(77Ya6DM)

44.925428 N 40.983915 E
(77Ya6DM)

52.855571 N 103.232513 E
(77Ya6VP)

67.613910 N 63.752342 E
(under construction)

FIGURE 28 - VORONEZH AT ORSK



The image above shows the Voronezh-VP array near Orsk, one of several such radars in operational use or under construction.

65.209966 N 57.285247 E
(Daryal—Image Shown)

52.848887 N 26.470524 E
(Volga)

FIGURE 29 – DARYAL AT PECHORA

The image above shows the Daryal bistatic array near Pechora.

SENSOR COMPLEXES

RUSSIA →

RADAR COMPLEXES

DNESTR/DNEPR/DAUGAVA RADAR SITES

52.874943 N 103.260566 E
(Dnestr)

52.877874 N 103.272584 E
(Dnepr—Image Shown)

46.603278 N 74.530860 E
(Dnepr)

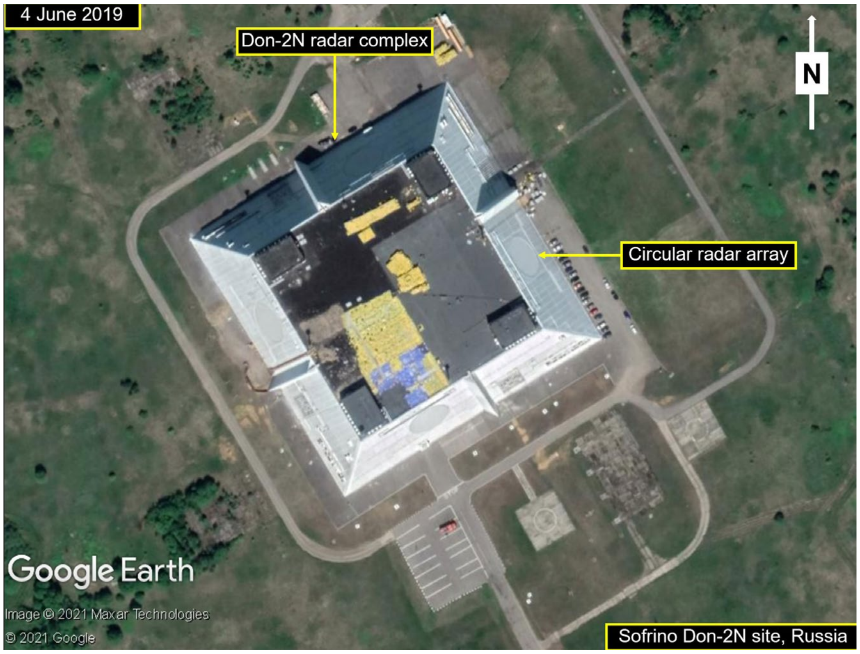
68.113720 N 33.910522 E
(Daugava)

FIGURE 30 - DNEPR SITE AT SARY SHAGAN

The image above shows a Dnepr radar array at Sary Shagan.

56.173299 N 37.769327 E
(Don-2N)

FIGURE 31 – DON-2N SITE AT SOFRINO



The image above shows the Don-2N radar, NATO codename Pill Box, near Sofrino outside of Moscow. It is a critical part of the A-135 ABM system.

55.219146 N 37.294505 E
(Dunai-3M)

FIGURE 32 – DUNAI-3M AT CHEKHOV

The image above shows a Dunai-3M radar at Chekhov, which was part of the A-135 ABM system.

SENSOR COMPLEXES

RUSSIA →

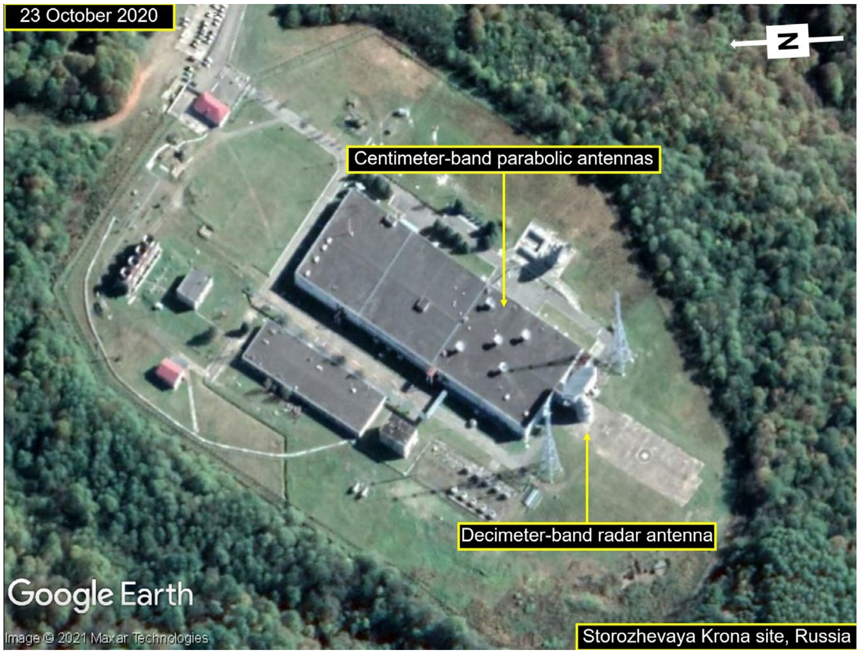
SPACE SURVEILLANCE COMPLEXES

KRONA SITES

43.826155 N 41.343355 E
(Radar—Image Shown)

42.935368 N 132.576247 E
(Radar)

FIGURE 33 - KRONA COMPLEX NEAR STOROZHEVAYA



The above image shows the Krona complex near Storozhevaya. Krona employs both electro-optical and radar sensors for satellite identification and tracking. Here you can see the decimeter and centimeter band radar antennas.

43.718100 N 41.227653 E
(30J6 Electro-optical)

FIGURE 34 – 30J6 COMPLEX NEAR STOROZHEVAYA

The above image shows the 30J6 component of the Krona complex near Storozhevaya, which contains the optical telescopes and lasers.

SENSOR COMPLEXES

RUSSIA →

SPACE SURVEILLANCE COMPLEXES

OKNO SITES

38.280551 N 69.224786 E

FIGURE 35 - OKNO COMPLEX NEAR NUREK

The above image shows the Okno complex near Nurek in Tajikistan. It is part of Russia's Centre for Outer Space Monitoring and uses a variety of electro-optical sensors to track space objects, mainly in the geosynchronous region.

SENSOR COMPLEXES

UNITED STATES →

SPACE SURVEILLANCE NETWORK

MAJOR RADAR AND OPTICAL SITES

41.752219 N, 70.538061 W
(Cod—Image Shown)

76.570308 N, 68.299256 W
(Thule)

64.290006 N, 149.191381 W
(Clear)

54.3616 N, 0.6697 W
(Fylingdales)

52.736644 N, 174.091617 E
(Cobra Dane)

48.724475 N, 97.899864 W
(PARCS)

30.573 N, 86.215 W
(Eglin)

8.723375 N, 167.718564 E
(Space Fence)

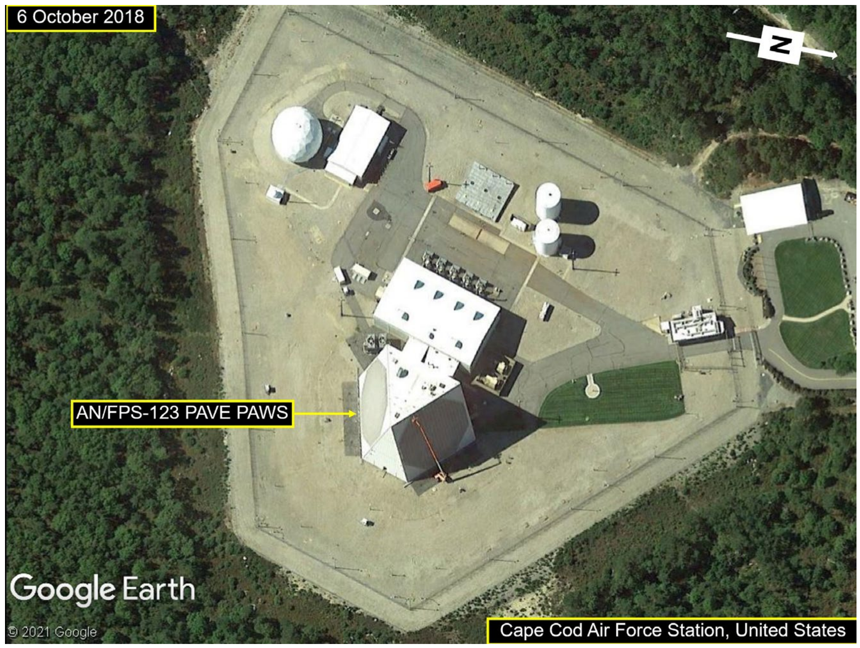
42.620033 N, 71.490289 W
(Lincoln Space Surveillance Complex)

9.394789 N, 167.47925 E
(Reagan Test Site)

21.816631 S, 114.165617 E
(Naval Communication Station Harold E. Holt)

20.7088 N, 156.2578 W
(Air Force Maui Optical and Supercomputing Observatory)

FIGURE 36 - CAPE COD MISSILE WARNING RADAR



The U.S. military operates multiple phased array radars with the primary purpose of missile warning but also with a space situational awareness secondary function. The above image shows one of these radars, the AN/FPS-123 PAVE PAWS, located at Cape Code Air Force Station in Massachusetts, from which it has coverage over much of the northeastern coast of the United States.

SENSOR COMPLEXES

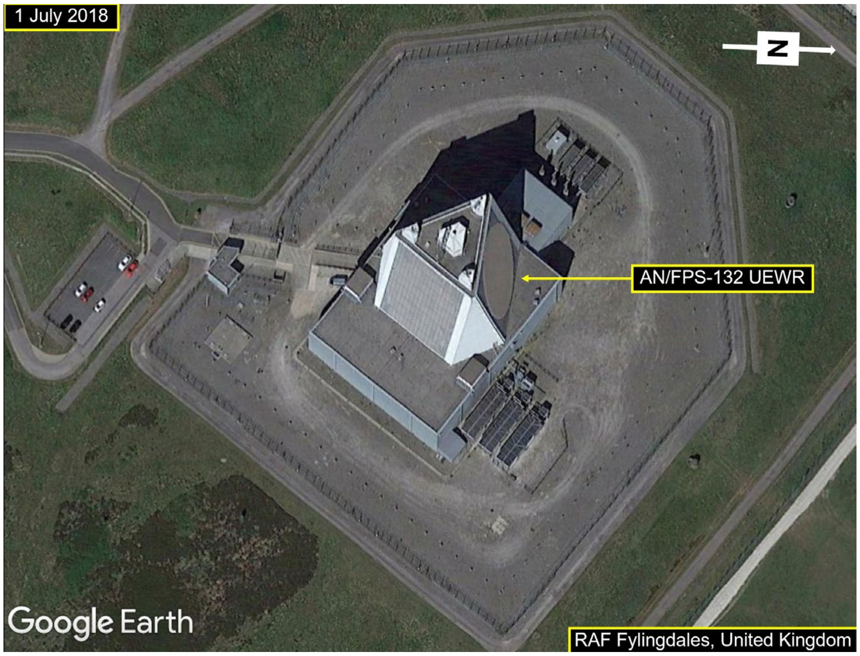
UNITED STATES →

SPACE SURVEILLANCE NETWORK

MAJOR RADAR AND OPTICAL SITES

54.3616 N, 0.6697 W
(Fylingdales—Image Shown)

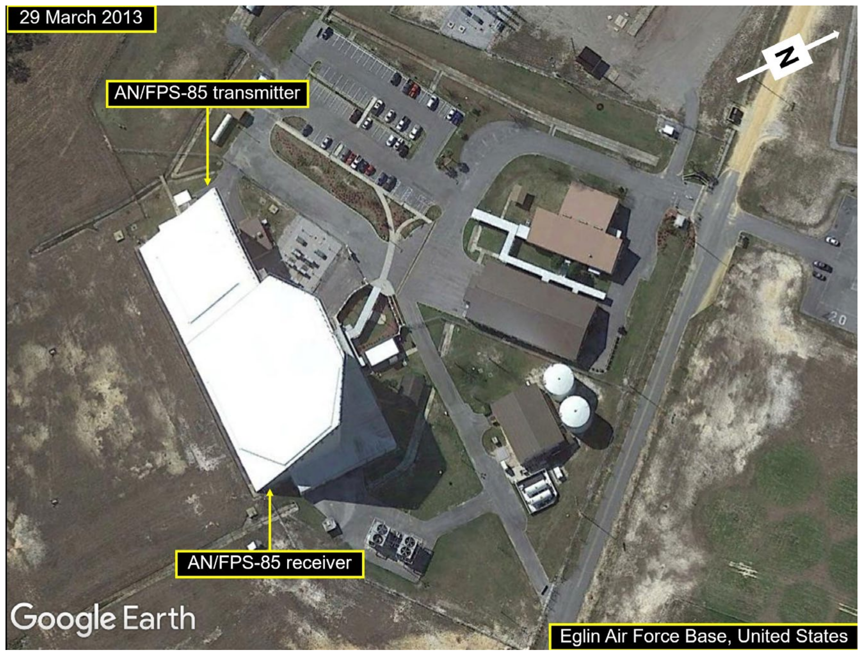
FIGURE 37 – FYLINGDALES MISSILE WARNING RADAR



The above image shows the AN/FPS-126 radar located at Royal Air Force Fylingdales in North Yorkshire, England. Note that the Fylingdales radar has three faces, giving it 360 degree coverage, compared to the two faces of the Cod radar.

30.573 N, 86.215 W
(Eglin—Image Shown)

FIGURE 38 – EGLIN SPACE SURVEILLANCE RADAR



The above image shows the AN/FPS-85 phased array radar located at Eglin Air Force Base in Florida. It has one face but can track objects at altitudes up to 36,000 kilometers.

SENSOR COMPLEXES

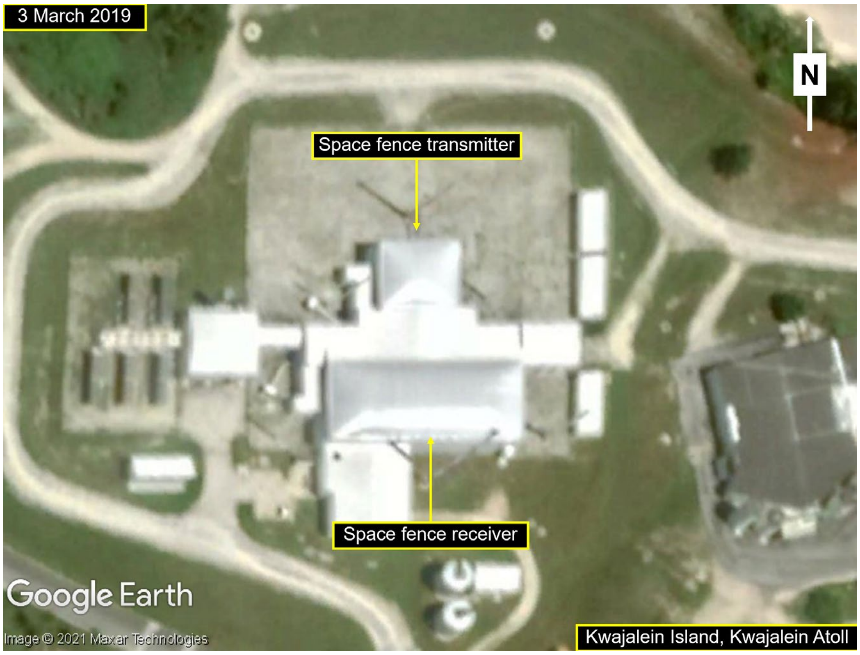
UNITED STATES →

SPACE SURVEILLANCE NETWORK

MAJOR RADAR AND OPTICAL SITES

8.723375 N, 167.718564 E
(Space Fence)

FIGURE 39 – S-BAND SPACE FENCE



The above image shows the recently-built S-Band Space Fence located on Kwajalein Atoll in the South Pacific. This system replaced the old Air Force Space Fence and is planned to track objects as small as a few centimeters in size out to 36,000 kilometers.

SENSOR COMPLEXES

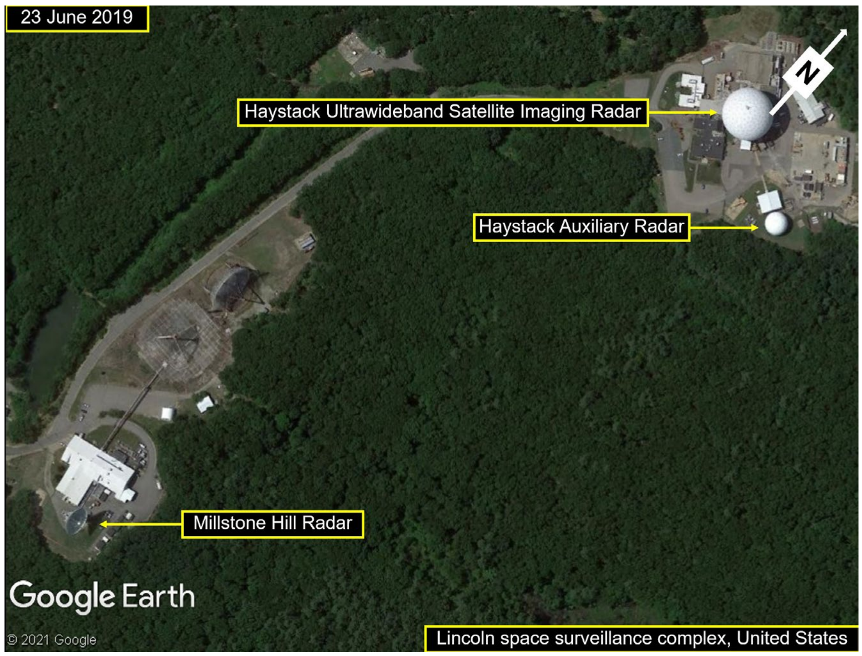
UNITED STATES →

SPACE SURVEILLANCE NETWORK

MAJOR RADAR AND OPTICAL SITES

42.620033 N, 71.490289 W
(Lincoln Space Surveillance Complex)

FIGURE 40 – LINCOLN SPACE SURVEILLANCE COMPLEX



The above image shows the Lincoln Space Surveillance Complex located near Boston, Massachusetts, which has multiple dish and phased array radars for tracking and characterizing space objects out to 36,000 kilometers.

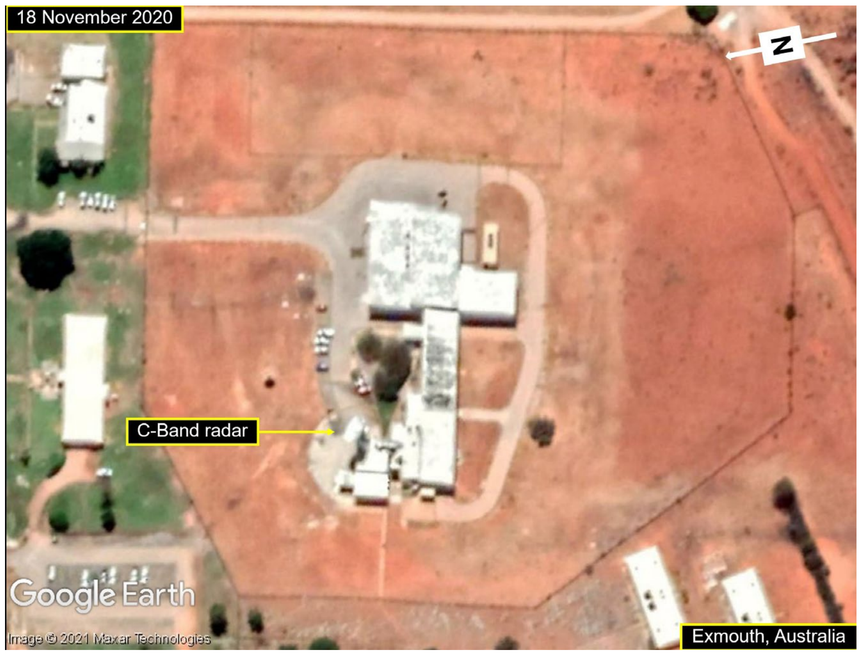
9.394789 N, 167.47925 E
(Reagan Test Site)

FIGURE 41 – REAGAN TEST SITE

The image above shows the Reagan Test Site on Kwajalein Atoll, which contains multiple radars that were originally used for missile defense testing and currently support both missile defense and SSA missions.

21.816631 S, 114.165617 E
(Naval Communication Station Harold E. Holt)

FIGURE 42 – HOLT C-BAND RADAR IN EXMOUTH



The image above shows the C-Band radar recently moved from Antigua Island in the Atlantic to Naval Communication Station Harold E. Holt near Exmouth, Western Australia, in order to augment the SSN's coverage in the Southern Hemisphere.

20.7088 N, 156.2578 W
(Air Force Maui Optical and Supercomputing Observatory)

FIGURE 43 – AIR FORCE MAUI OPTICAL AND SUPERCOMPUTING OBXSERVATORY

The image above shows the Air Force Maui Optical and Supercomputing Observatory located on the island of Maui in Hawaii. It includes multiple electro-optical sensors for tracking objects in deep space, including the Advanced Electro Optical System (AEOS) telescope that can image objects in LEO.

SENSOR COMPLEXES

FRANCE →

RADAR COMPLEX GRAVES

47.3480 N 5.5151 E
(transmitter)

FIGURE 44 – GRAVES RADAR TRANSMITTER

The image above shows the Grand Réseau Adapté à la Veille Spatiale (GRAVES) system operated by the French military for SSA. It is a bistatic radar, consisting of a geographically separated transmitter and receiver and is capable of tracking objects in LEO.

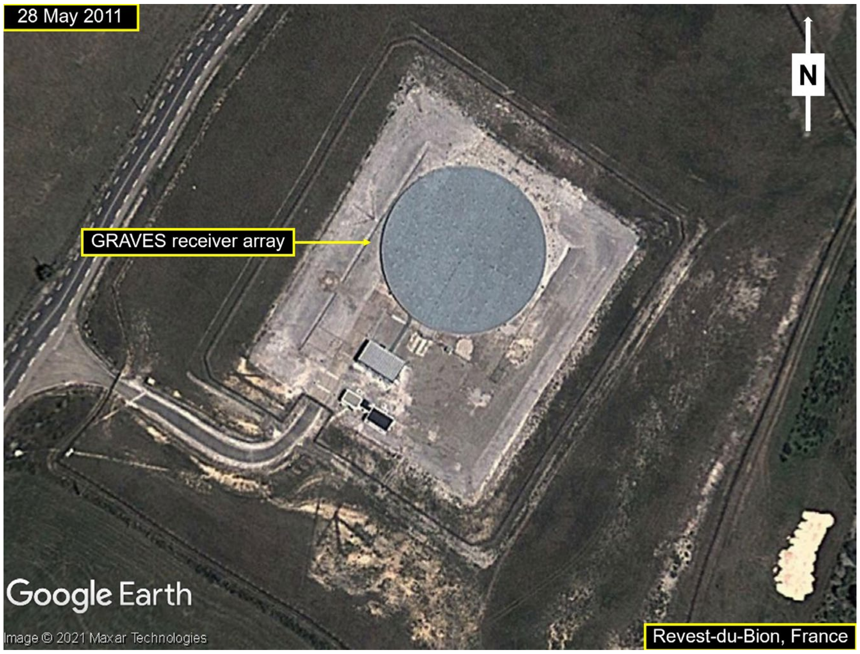
SENSOR COMPLEXES

FRANCE →

RADAR COMPLEX GRAVES

44.0715 N 5.5346 E
(receiver)

FIGURE 45 – GRAVES RADAR RECEIVER



The image above shows the Grand Réseau Adapté à la Veille Spatiale (GRAVES) system operated by the French military for SSA. It is a bistatic radar, consisting of a geographically separated transmitter and receiver and is capable of tracking objects in LEO.

SENSOR COMPLEXES

INDIA →

RADAR COMPLEX

GREEN PINE/
SWORDFISH RADAR SITES

19.854052 N 85.969496 E
(Garhbangor—Image Shown)

13.195549 N 78.173603 E
(Gopasandra)

FIGURE 46 – SWORDFISH RADAR NEAR GARHBANGOR

The image above shows the Swordfish radar installation near Garhbangor.

SENSOR COMPLEXES

IRAN →

SPACE SURVEILLANCE COMPLEX

DELIJAN

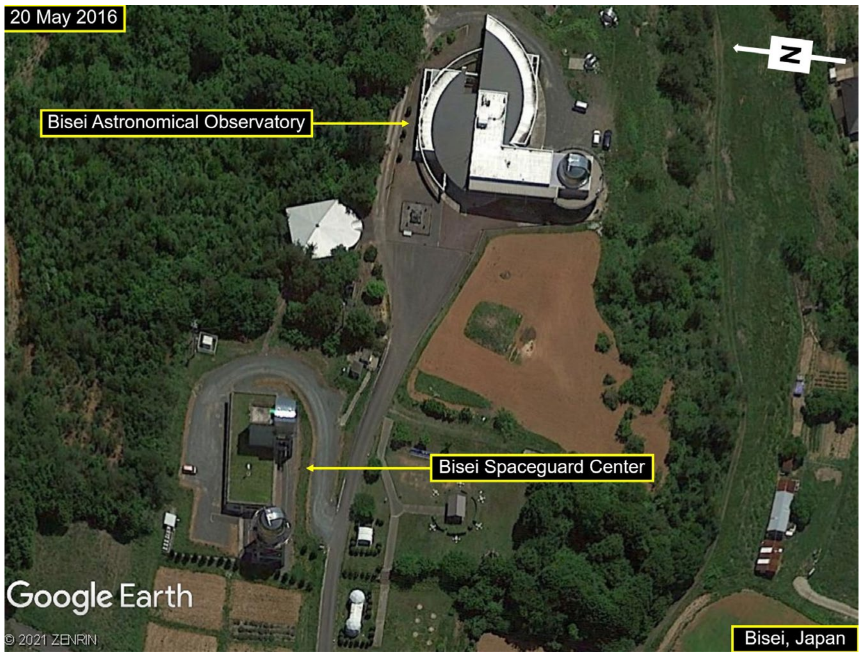
34.119728 N 50.877829 E

FIGURE 47 – DELIJAN SPACE TRACKING CENTER

The image above shows the Delijan Space Tracking Center, located in Varn, Iran, about 200 kilometers south of Tehran. The site includes multiple radar and electro-optical sensors for tracking space objects.

34.672225 N 133.544089 E
(Bisei)

FIGURE 48 – BISEI SPACEGUARD CENTER



The image above shows the Bisei Spaceguard Center at Bisei-chō in Okayama, which is Japan's main optical tracking facility for SSA.

SENSOR COMPLEXES

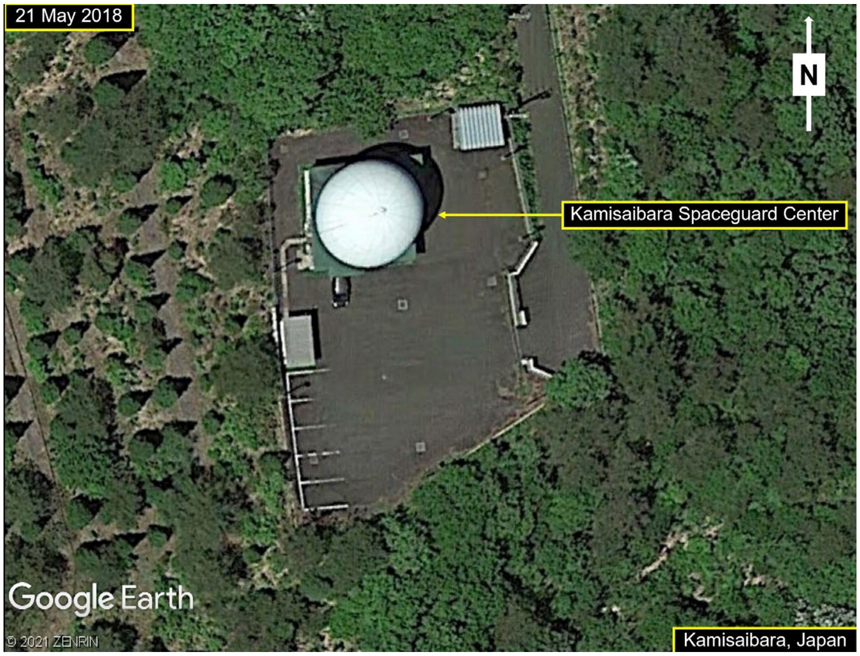
JAPAN →

SPACE SURVEILLANCE COMPLEX

SPACEGUARD CENTER

35.3123 N 133.941364 E
(Kamisaibara)

FIGURE 49 – KAMISAIBARA SPACEGUARD CENTER



The image above shows Kamisaibara Spaceguard Center, which is also in Okayama, and is the location of a radar that can track objects in LEO.

Secure World Foundation

525 Zang Street,
Broomfield, Colorado 80021
—
+1 305.554.1560

1779 Massachusetts Avenue NW,
Washington, DC 20036
—
+1 202.568.6212

info@swfound.org | swfound.org | @SWFoundation