GLOBAL COUNTERSPACE CAPABILITIES

An Open Source Assessment

> 04 | 2024

SECURE WORLD FOUNDATION

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 mission of the Secure World Foundation is to work with governments, industry, international organizations, and civil society to develop and promote ideas and actions to achieve the secure, sustainable, and peaceful uses of outer space benefiting Earth and all its peoples.

ABOUT THE EDITORS

Dr. Brian Weeden
Chief Program Officer

Dr. Brian Weeden is the Chief Program Officer 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 US 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 US Congress.

Ms. Victoria Samson
Chief Director,
Space Security and Stability

Ms. Victoria Samson is the Chief Director, Space Security and Stability for Secure World Foundation and has over 25 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 space security matters. She is also the head of the International Astronautical Federation’s task force on security and a member of the Space Security Working Group of the National Academies of Sciences, Engineering, and Medicine’s Committee on International Security and Arms Control.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

AAD
Advanced Area Defense

ABL
Airborne Laser

ABM
Anti-Ballistic Missile

ACCRES
Advisory Committee on Commercial Remote Sensing

ADF
Australian Defence Force

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 Co-operation Organization

APSSO
Asia-Pacific Space Science Observatories

APT
Advanced Persistent Threat

ASAT
Antisatellite

ASDF
Aerospace Self-Defence Force

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

CMC
Central Military Commission

CMOS
Complementary Metal-oxide Semiconductor

CNE
Computer Network Exploitation

CNES
Centre national d'études spatiales

COIL
Chemical Oxygen Iodine Laser

COMINT
Communications Intelligence

COMSAT
Communications Satellite

CSpOC
Combined Space Operations Center

CSRS
Counter Surveillance and Reconnaissance System

DA-ASAT
Direct-Ascent ASAT

DARC
Deep Space Advanced Radar Capability

DARPA
Defense Advanced Research Projects Agency

DART
Demonstration for Autonomous Rendezvous Technology

DAAS
Data as a Service

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

DSS
Defence Space Strategy

EAGLE
ESPA Augmented Geostationary Laboratory Experiment

ECS
Environmental Control Systems

EELV
Evolved Expendable Launch Vehicle

EO
Earth Observation

EOSAT
Electronic Ocean Surveillance Satellite

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

HEO
Highly Elliptical Orbit

HIMARS
High Mobility Artillery Rocket System

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

IMDO
Israel Missile Defense Organization

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

JASDF
Japanese Air Self-Defense Force

JAXA
Japan Aerospace Exploration Agency

JDAM
Joint Direct Attack Munition

JFSCC
Joint Force Space Component Command

JICSpOC
Joint Interagency Combined Space Operations Center

JNWC
Joint Navigation Warfare Center

JSpOC
Joint Space Operations Center

JTF-SD
Joint Task Force Space Defense

KARI
Korea Aerospace Research Institute

KCNA
Korean Central News Agency

KIAM
Keldysh Institute of Applied Mathematics

KKV
Kinetic Kill Vehicle

KRIT
Korea Research Institute for Defense Technology Planning and Advancement

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

MDO
Multidomain Operations

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

MUBLCOM
Multiple Path Beyond Line of Site Communication

NASA
National Aeronautics and Space Administration

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 Air Missions

NPT
Nuclear Non-Proliferation Treaty

NRL
Naval Research Laboratory

NSA
National Security Agency

NSDC
National Space Defense Center

NSS
National Space Strategy

OCS
Offensive Counterspace

OKN
Integrated Observation Complex

OSC
Offensive Space Control

OTV
Orbital Test Vehicle

PAD
Prithvi Air Defence

PARCS
Perimeter Acquisition Radar Attack System

PAVE PAWS
Precision Acquisition Vehicle Entry 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

RAF
Royal Air Force

RAT
Remote Access Tool

RDT&E
Research, Development, Testing, and Evaluation

RF
Radiofrequency

RKA
Relativistic Klystron Amplifier

RORSAT
Radar Ocean Reconnaissance Satellite

RPO
Rendezvous and Proximity Operations

SAASM
Selective Availability Anti-Spoofing Module

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

SFIA
Space Force Intelligence Activity

SHF
Super-High Frequency

SIGINT
Signals Intelligence

SIP
Satellite Interceptor Program

SKKP
Центр контроля космического пространства, tr. Tsentr kontrolya kosmicheskogo prostranstva ("Space Surveillance System")

SLBM
Submarine-launched Ballistic Missile

SLR
Satellite Laser Ranging

SLV
Space Launch Vehicle

SPR
Space Strategic Portfolio Review

SSA
Space Situational Awareness

SSC
Space Systems Command

SSN
Space Surveillance Network

SSS
Space Surveillance System

SST
Space Surveillance Telescope

SWAC
Space Warfighting Analysis Center

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

UKSA
United Kingdom Space Agency

UKSpOC
UK Space Operations Centre

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

XGEO
Beyond Geostationary Earth Orbit

YODA
Yeux en Orbite pour un Démonstrateur Agile

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 against satellites in current military operations.** The following provides a more detailed summary of each country's capabilities.

	US	RUSSIA	CHINA	INDIA	AUS.	FRANCE	IRAN	ISRAEL	JAPAN	N. KOREA	S. KOREA	UK
LEO Direct Ascent	Some	Some	Significant	Some	None	None	None	None	None	None	None	None
MEO/GEO Direct Ascent	Some	Some	Some	None	None	None	None	None	None	None	None	None
LEO Co-Orbital	Some	Significant	Some	None	None	None	None	None	None	None	None	None
MEO/GEO Co-Orbital	Some	Some	Some	None	None	None	None	None	None	None	None	None
Directed Energy	Some	Some	Some	None	None	Some	None	None	None	None	None	None
Electronic Warfare	Significant	Significant	Significant	Some	Some	Some	Some	Significant	Some	Some	None	None
Space Situational Awareness	Significant	Significant	Significant	Some	Some	Some	Some	Some	Some	Some	Some	Some

LEGEND: NONE ● SOME ■ SIGNIFICANT ▲ UNCERTAIN ? NO DATA –

1 – THE UNITED STATES

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

LEGEND: NONE ● SOME ■ SIGNIFICANT ▲ UNCERTAIN ? NO DATA –

The United States has conducted multiple tests of technologies for close approach and rendezvous in both LEO and GEO, along with tracking, targeting, and hit-to-kill (HTK) intercept technologies that could lead to a co-orbital antisatellite (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 direct ascent antisatellite (DA-ASAT) program, it does have operational midcourse missile defense interceptors that have been demonstrated in an ASAT role against a low LEO satellite. 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 electronic warfare (EW) offensive counterspace system, the Counter Communications System (CCS), which is deployed globally to provide uplink jamming capability against geostationary communications satellites. The United States has also initiated a program called Meadowlands to upgrade the CCS capabilities. Through its Navigation Warfare program, the United States has the capability to jam and interfere with the civil signals of global navigation satellite services (GNSS) 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 could jam military GNSS signals as well, although the effectiveness is difficult to assess based on publicly available information. The effectiveness of US 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 United States operationalizing them for counterspace applications. With its Satellite Laser Ranging (SLR) sites and defense research facilities, the United States possesses low-power laser systems with the capability to dazzle, and possibly blind, Earth observation (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 directed energy weapons (DEW) capability. The Missile Defense Agency (MDA) is planning to conduct research into the feasibility of DEW for defending against ballistic missiles and the Space Force has expressed an interest in a directed energy architecture in general (not necessarily space-based). 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.

The United States currently possesses the most advanced SSA capabilities in the world, particularly for military applications. US 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 US 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 current US military doctrine includes offensive and defensive military force and is focused on suppressing adversary uses of space in an armed conflict while protecting the United States' ability to use space.

The United States recently underwent a major reorganization of its military space activities as part of a renewed focus on space as a warfighting domain. Since 2014, US 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 US Space Command (USSPACECOM) and the creation of the US Space Force (USSF), which assumed the responsibilities of US Strategic Command for space warfighting and Air Force Space Command (AFSPC) for operating, training, and equipping of space forces, respectively. To date, the missions of these new organizations are largely a continuation of previous military space missions, although some have advocated for expanding their focus to include cislunar activities and more offensive weapons. It is possible that the United States has also begun developing new offensive counterspace capabilities, although the United States has publicly stated it will not test destructive DA-ASAT weapons. The United States also continues to hold annual space wargames and exercises that increasingly involve close allies and commercial partners.

2 — RUSSIA

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

LEGEND: NONE ● SOME ■ SIGNIFICANT ▲ UNCERTAIN ? NO DATA –

There is strong evidence that Russia has embarked on a set of programs since 2010 to regain offensive 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 match 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 has long had the potential for a DA-ASAT capability through its historical ballistic missile defense capabilities and had DA-ASAT development programs in the past that never fully became operational. In November 2021, after more than a decade of development and testing, Russia successfully demonstrated a DA-ASAT capability against a LEO satellite. It is unclear whether this system, the Nudol, will become operational soon, and it does not appear to have the capability to threaten targets beyond LEO.

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 (PGMs), but has no publicly known capability to interfere with the GPS satellites themselves using radio frequency 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 current military campaigns, as well as using it within 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 a mobile ground-based laser dazzler system, Peresvet, that is linked to protection of their road mobile intercontinental ballistic missile force. Russia may have revived a legacy program whose goal is to develop an aircraft-borne laser system for targeting the optical sensors of imagery reconnaissance satellites, although there is no indication that an operational capability has been achieved. Although not their intended purpose, Russian ground-based satellite laser ranging (SLR) facilities could be used to dazzle the sensors of optical imagery satellites. There is no indication that Russia is developing, or intending to develop, high-power space-based laser weapons.

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 maintains a catalog of Earth-orbiting space objects in LEO that is somewhat smaller than that of the United States but 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 US space assets by fielding a number of ground-, air-, and space-based offensive capabilities. Russia has recently reorganized 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.

3 — CHINA

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

LEGEND: NONE ● SOME ■ SIGNIFICANT ▲ UNCERTAIN ? NO DATA –

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, 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. 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 (medium Earth orbit, or 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.

China is likely to have significant EW counterspace capabilities against 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 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 five 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. 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 aids 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, unofficially 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 2016, China reorganized its space and counterspace forces, as part of a larger military reorganization, and placed them in a new major force structure that also has control over electronic warfare and cyber. China's considerable investment in developing and testing counterspace capabilities, as detailed in this chapter, suggest they see space as a domain for future conflicts, whether or not that is officially stated. 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 US aggression. There is no public evidence of China actively using destructive counterspace capabilities in current military operations, although it is likely they are using SSA and electronic warfare in at least some support roles.

4 — INDIA

	R&D	TESTING	OPERATIONAL	USE IN CONFLICT
LEO Direct Ascent	SOME	SOME	–	NONE
MEO/GEO Direct Ascent	–	–	–	NONE
LEO Co-Orbital	–	–	–	NONE
MEO/GEO Co-Orbital	–	–	–	NONE
Directed Energy	SOME	–	–	NONE
Electronic Warfare	SOME	SOME	?	?
Space Situational Awareness	SOME	SOME	?	?

LEGEND: NONE ● SOME ■ SIGNIFICANT ▲ UNCERTAIN ? NO DATA –

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 of space and creating explicit military space capabilities. India's military has developed indigenous missile defense and long-range ballistic missile programs that could lead to DA-ASAT capabilities, should the need arise. India demonstrated its ASAT capability in March 2019 when it destroyed one of its satellites. While India continues to insist that it is against the weaponization of space, India may be moving toward an offensive counterspace posture. India is reportedly in the early stages of working on directed energy weapons.

6 — AUSTRALIA

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

LEGEND: NONE ● SOME ■ SIGNIFICANT ▲ UNCERTAIN ? NO DATA –

Australia is a relative newcomer in space, although it has long played a support role by hosting ground infrastructure for satellite communications and command and control. Recently, however, Australia has been laying the groundwork for more indigenous space capabilities, including military. It has recently started a military space organization, is building out a policy framework for its military space priorities, is putting concerted efforts and resources into building its own SSA capabilities, is examining an EW capability for its Department of Defence, and is looking into non-destructive ways in which to interfere with enemy satellites.

7 — FRANCE

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

LEGEND: NONE ● SOME ■ SIGNIFICANT ▲ UNCERTAIN ? NO DATA –

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 active defense against threats. While some French officials suggested machine guns on satellites, the actual plan calls for ground-based lasers for dazzling and satellites equipped for on-orbit inspections and also with offensive lasers. In 2021 and 2022, France carried out military exercises, codenamed "ASTERX," in outer space, testing the capabilities of its Space Command, as part of France's evolving goal to be the world's third-largest spatial power.

8 — IRAN

	R&D	TESTING	OPERATIONAL	USE IN CONFLICT
LEO Direct Ascent	–	–	–	NONE
MEO/GEO Direct Ascent	–	–	–	NONE
LEO Co-Orbital	–	–	–	NONE
MEO/GEO Co-Orbital	–	–	–	NONE
Directed Energy	–	–	–	NONE
Electronic Warfare	SIGNIFICANT	SIGNIFICANT	SOME	SOME
Space Situational Awareness	SOME	SOME	?	?

LEGEND: NONE ● SOME ■ SIGNIFICANT ▲ UNCERTAIN ? NO DATA –

Iran has a nascent space program, 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 motivation for doing so at this point. Iran's military appears to have an independent ability to launch satellites, separate from Iran's civil space program. Iran has not demonstrated any ability to build homing kinetic kill vehicles, and its ability to build nuclear devices is still constrained. Iran has demonstrated an EW capability to persistently interfere with the broadcast of commercial satellite signals, although its capacity to interfere with military signals is difficult to ascertain.

9 — ISRAEL

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

LEGEND: NONE ● SOME ■ SIGNIFICANT ▲ UNCERTAIN ? NO DATA –

In 1988, Israel became the eighth country to be able to launch its own satellite into orbit. It has maintained a space program that has largely been civil in nature and co-developed a missile defense system that has been until recently strictly for endoatmospheric interception of rockets. However, in recent years Israel has moved to expand its military space program and there is evidence it has developed counterspace capabilities. These include the recent demonstration of an exoatmospheric missile defense intercept capability and use of EW in active military conflicts. It is possible Israel has additional counterspace capabilities that are not publicly visible or documented.

10 – JAPAN

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

LEGEND: NONE ● SOME ■ SIGNIFICANT ▲ UNCERTAIN ? NO DATA –

Japan has long been a well-established space actor and its space activities have historically been 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 the development of enhanced SSA capabilities to support military and civil applications. While Japan does not have any acknowledged offensive counterspace capabilities, it is 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.

11 – NORTH KOREA

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

LEGEND: NONE ● SOME ■ SIGNIFICANT ▲ UNCERTAIN ? NO DATA –

North Korea has no demonstrated capability to mount kinetic attacks on space assets: neither a DA-ASAT nor a co-orbital system. In its official statements, North Korea has not mentioned ASAT operations or intent, suggesting that there is no clear doctrine in Pyongyang's thinking at this point. North Korea does not appear highly motivated to develop dedicated counterspace assets, though certain capabilities in its ballistic missile program might be eventually evolved for such a purpose. North Korea has exhibited the capability to jam civilian GPS signals within a limited geographical area. Their capability against US 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.

12 — SOUTH KOREA

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

LEGEND: NONE ● SOME ■ SIGNIFICANT ▲ UNCERTAIN ? NO DATA –

Over the last several years, South Korea has had a growing focus on military space capabilities. It is working to enhance the space capabilities of its Air Force through the establishment of a Space Operations Center, cooperating with the United States on sharing SSA capabilities, and developing its own longer-range ballistic missiles and space launch vehicles; it also has expressed interest in developing its own reversible counterspace capabilities.

13 — THE UNITED KINGDOM

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

LEGEND: NONE ● SOME ■ SIGNIFICANT ▲ UNCERTAIN ? NO DATA –

The United Kingdom has long played a supporting role in military space activities through its participation in NATO and its bilateral relationship with the United States. Over the past few years, the United Kingdom has begun to add additional elements to increase its indigenous military space capabilities, primarily in SSA and policy, organization, and doctrine. To date, the United Kingdom has not publicly announced any specific plans to develop offensive counterspace capabilities.

14 — CYBER CAPABILITIES

Multiple countries possess cyber capabilities that could be used against space systems; however, actual evidence of cyber attacks in the public domain is limited. The United States, Russia, China, North Korea, Israel 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 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 and nearly all have gone after the end user segment and not satellites themselves. The largest was a cyber attack by Russia against the user segment of Viasat's commercial satellite broadband service in Europe, which coincided with the first day Russian forces entered Ukraine in February 2022.

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 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.

2024 ADDITIONS

>

The following are brief summaries of the major additions for the 2024 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 — The United States /

- Revised assessment of US efforts to develop new offensive counterspace capabilities (1-01)
- Added history of the X-37B program and details about the end of OTV-6 and the current OTV-7 missions (1-04)
- Added retirement of two original GSSAP satellites, launch of two new GSSAP satellites to the GEO region, and information on non-US satellites visited by GSSAP (1-09)
- Added launch of Tetra-1 payload to the GEO region, which has been used in training maneuvers as part of Scarlet Star (1-11)
- Added new progress on the Aegis Ashore site in Poland (1-17)
- Added CCS operations by the Air National Guard and revised the number of operational CCS systems (1-21)
- Revised expected completion date and budget forecast for the Meadow lands upgrade to CCS (1-21)
- Added the second and third iteration of the USSF Black Skies live fire space jamming exercises and the Red Skies orbital warfare training scenario exercise (1-22)
- Added further delays to the OCX ground system for GPS-III (1-23)
- Added additional GPS jamming exercises conducted by the US military in several US states (1-23)
- Added details about the MOSSAIC program to upgrade and expand US ground-based optical telescopes for SSA (1-31)
- Added announcement of US, UK, and Australian partnership in the DARC program to develop new deep space tracking radars (1-31)

- Added mention of Space System Commands' Project Apollo to tackle critical SSA challenges (1-32)
- Added launch of the first SILENT BARKER payload in the GEO region and clarification of the differences between SILENT BARKER and GSSAP (1-32)
- Added launch of three SpRCO payloads to the GEO region to assist with threat assessment collection (1-32)
- Added details on the US capabilities for space weather prediction and warning (1-34)
- Revised US national space policy and doctrine on counterspace to incorporate the new changes made in Joint Publication 3-14 and Space Doctrine Publication 3-0 (1-36)
- Added changes to the relationship between USSPACECOM, USSTRATCOM, and USNORTHCOM as dictated by the 2023 revision to the Unified Combatant Plan (1-37)
- Added the DA-ASAT missile testing moratorium initiative (1-38)
- Added CSO Saltzman's new Competitive Endurance theory of success for the Space Force (1-38)
- Added the DoD's Space Policy Review (1-39)
- Added Italy, Japan, and Norway joining the CSpO initiative (1-39)
- Added reorganization of USSPACECOM by merging JTF-SD and JTF-CFSCC into US Space Forces-Space Command (1-40)
- Added activation of the 75th Intelligence, Surveillance, and Reconnaissance Squadron as the first targeting unit supporting the USSF (1-41)
- Added ongoing debate over creating a Space National Guard (1-42)
- Added US Army's new Multidomain Operations memo on how it plans to leverage space (1-42)
- Added details on the 2023 Schriever Wargame participants (1-43)
- Added USSOUTHCOM holding its first defensive space control operation as part of the Resolute Sentinel 23 exercise (1-43)

---

02 — Russia /

- Clarified that only the first two Almaz space stations carried cannons (2-04)
- Added launch of Cosmos 2565 and subsequent deployments of Cosmos 2566 and Object D (2-11)
- Updated orbital history of Luch (Olymp-K) and further details on its likely signals intelligence collection mission (2-13)
- Added launch of Luch Olymp 2 satellite and its subsequent RPO with several US and European communications satellites in GEO (2-13)
- Added RPO between Cosmos 2562 and Resurs-P in LEO (2-15)
- Added reports of Russia developing a new co-orbital weapon based on a nuclear bomb (2-15)
- Correct Burevestnik as being linked to a co-orbital ASAT program and not a DA-ASAT (2-17)
- Removed two presumed Nudol flight tests (April and June 2021) that did not actually take place (2-19)

- Added reports of GPS jamming in Eastern Ukraine impacting military systems (2-25)
- Added increased jamming and spoofing of GNSS in the Baltic Sea affecting civil aviation (2-26)
- Added report of Russian use of Tobol EW system against Starlink (2-26)
- Added Russian jamming of commercial communications satellites over Eastern Ukraine (2-27)
- Added new Razvyazka phased array radar near Chekhov reaching operational status (2-34)
- Added information on the completion of the Milky Way upgrades at the OKN complex in the Russian Far East (2-36)

03 — China /

- Added NEO-01 satellite that is reported to have conducted an experimental capture of a tethered object using a deployed net (3-04)
- Added details about the end of the second flight of China's Shenlong spaceplane and the launch of the third flight (3-05)
- Updated RPO activities of the SJ-17 and TJS-3 satellites in GEO (3-06)
- Added launch of the SJ-23 satellite to GEO and its release and RPO of another space object (3-09)
- Added potential new test of the DN-3 DA-ASAT system in April 2023 (3-15)
- Added discussion of potential space-based jamming of satellite capabilities (3-18)
- Added reports of the laser facility at Bofu having its roof opened during overflights of US commercial remote sensing satellites (3-19)
- Added reports of advances in power systems to support high power microwave beam weapons (3-20)
- Clarified the locations of China's six known phased array missile warning radars (3-21)
- Added Chinese-Egyptian agreement to host a new satellite tracking station in Egypt (3-22)
- Clarified distinction between China's official views on space warfighting and our assessment based on their observed programs and activities (3-23)
- Added new information on the organization of the SSF for counterspace command and control (3-25)

04 — India /

- Reorganized chapter to lead with co-orbital ASAT technologies (4-01)
- Added second flight of the Indian spaceplane (4-01)
- Added reports of new investments by the Indian military into ground-based offensive EW capabilities (4-05)
- Added new investments by the Indian military and DRDO on directed energy weapons (4-05)
- Updated the timeline for the Project NETRA SSA program (4-05)

- Added publication of the first ever Indian National Space Policy (4-05)
- Added comments by senior military leadership on the value of future space-based offensive platforms (4-07)

06 — Australia /

- Added Australian purchase of a CCS offensive counterspace EW system from the US (6-01)
- Added announcement of Australia hosting the first DARC deep space tracking site (6-01)
- Added Australia pledge not to conduct destructive DA-ASAT missile tests (6-02)
- Added release of the Australian Strategic Defense Review (6-03)

07 — France /

- Reorganized chapter to lead with co-orbital ASAT technologies (7-01)
- Added report of France's willingness to share technology on counterspace EW capabilities with Saudi Arabia (7-01)
- Added reports of French authorities discovered multiple GNSS jammers near the Merville airport (7-01)
- Added details on the FLAMHE program to place laser-armed satellites in GEO and the BLOOMLASE program to develop ground-based laser dazzlers (7-02)
- Added telescope at Les Makes Observatory (7-03)
- Added CNES contract with ArianeGroup to develop a network of ground and space-based SSA sensors (7-03)
- Added French pledge not to conduct destructive DA-ASAT missile tests (7-04)

08 — Iran /

- Reorganized chapter to lead with co-orbital ASAT technologies (8-01)
- Updated details on the satellites Iran has been able to place in space (8-01)
- Added first successful launch of the Simorgh SLV by the Iranian Space Agency to place the Kayhan-2, Hatef-1, and Mehda satellites in LEO (8-02)
- Added third successful launch of the Qassed SLV by the IRGC to place the Noor-3 satellite in LEO (8-03)
- Added second successful launch of the Qaem-100 SLV by the IRGC to place the Sorayya satellite in LEO and announcements on the development of the upgraded Qaem-105 and Qaem-120 version (8-03)
- Added reports of GPS interference affecting commercial aircraft, which was traced to outside of Tehran (8-04)
- Added announcement of the Aerospace Force's Space Command within the IRGC (8-05)

09 — Israel /

- Added country for the first time

10 — Japan /

- Reorganized chapter to lead with co-orbital ASAT technologies (10-01)
- Added new partnership between Northrop Grumman and IHI to develop small, highly maneuverable satellites for SSA and to protect satellites in GEO (10-02)
- Added Japan's pledge not to conduct destructive DA-ASAT missile tests (10-03)
- Added new Space Security Initiative that outlines Japan's strategy for responding to space threats (10-04)

11 — North Korea /

- Re-organized chapter to lead with co-orbital ASAT technologies (11-01)
- Added details on the assessed capabilities of the Malligyong-1 remote sensing satellite (11-01)
- Added three successful flight tests of the Hwasong-17 mobile ICBM (11-02)
- Added the first unsuccessful and first successful launch of the Chollima-1 SLV that placed the Malligyong-1 satellite in LEO (11-03)

12 — South Korea /

- Added the first successful flight of the Nuri SLV that placed eight satellites in LEO (12-01)
- Added South Korea's pledge not to conduct destructive DA-ASAT missile tests (12-02)
- Added increase budget for space systems, including a new SLV and space defense programs (12-03)
- Added table-top exercise on how to respond to dangers from space and interagency coordination (12-03)

13 — The United Kingdom /

- Added request to industry for bids on developing a new ground-based tracking telescope in Cyprus (1301)
- Added UK creating the Joint Task Force Space-Defense Commercial Operations Cell (13-01)
- Added announcement of the UK joining the US and Australia in the DARC deep space tracking radar program (13-01)
- Added the UK's pledge not to conduct destructive DA-ASAT missile tests (13-03)

14 — Cyber /

- Added Killnet hacktivist denial of service attack on Starlink (14-06)
- Added cyber attack on Russian satellite communications provider Dozor-Teleport (14-06)
- Added fifth category of cyber attacks against satellites themselves and “hack-a-thon” contests by the USAF and ESA to attack simulated or real satellites (14-08)
- Added new research from Blackhat 2023 on cyber security weaknesses of academic and scientific cubesats (14-08)
- Added reports of classified US assessment that China is developing sophisticated cyber weapons to seize control of satellites during wartime (14-09)

16 — Appendix II /

- Fixed coordinates of Plesetsk Space Launch Center Site 133 (16-6)
- Added imagery of the Wenchang Space Launch Center on Hainan Island (16-15)
- Added imagery of the Razvyazka radar at Chekhov (16-47)

ACKNOWLEDGE-MENTS

Catherine Dill

Gilles Doucet

Kylee Dickinson

Jeffrey Edmonds

Laura Grego

Marissa Martin

Louison Mazeaud

Brandon Kelley

Jonathan McDowell

Sean O'Connor

Pavel Podvig

Kevin Pollpeter

Robert Ronci

Tamara Tanso

Seth Walton

Josh Wolny

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.

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 the COMSPOC Corporation 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, nor is space security and stability something that only matters to geopolitical rivals. 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 here on Earth, as everyone on this planet is a user of space data in some form. 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 the 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 hoped to. 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.

Brian Weeden and Victoria Samson

INTRODUCTION

>

The space domain is undergoing a significant set of changes. A growing number of countries and commercial actors are getting involved in space, resulting in more innovation and benefits on Earth but also more congestion and competition in space. From a security perspective, an increasing number of countries are looking to use space to enhance their military capabilities and national security. Most of the space applications being worked on 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 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 for a limited time and location. 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. Anti-satellite (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 capabilities to support 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 attacks. 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 by 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, the 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 the development of counterspace capabilities by several countries. We decided to examine five 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 radio frequency 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 2024.**

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 three-digit incrementing launch number of that year, and up to a three-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 US military in its public satellite catalog, often referred to as the satellite number or satno, which increments by one for each new object cataloged. In this text, the 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 and for which there is public evidence of these efforts.. 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 could be much more widely proliferated than indicated herein this report. 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' concerns 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.

In 2022, we did a major restructuring to better highlight the scope of different countries' counterspace activities. The report is now divided into three main sections. Section 1 includes countries that have conducted destructive ASAT tests in space, in chronological order by year of their first test, and ends with an assessment of the space debris created by these tests. Section 2 includes countries that have significant counterspace R&D programs but have not yet done a destructive test. Section 3 focuses on cyber capabilities, given that they are exceedingly difficult to assess on a per-country level based on open-source data. Finally, the report includes two Appendices: one with tables of historical ASAT testing in space, and a second with satellite imagery of major launch, testing, and other facilities discussed in the report.

Countries That Have Conducted Destructive ASAT Tests

1

38.9072°N

01

THE UNITED STATES

77.0369°W

The United States currently has the most advanced military space capabilities in the world although the relative gap with China is narrowing. 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 US 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 to counter specific Soviet military space capabilities, such as the ability to use satellites to target US 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, deliberate 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. The United States is likely developing new offensive counterspace capabilities, to deny an adversary their own space capabilities in the event of a future conflict, although these are unlikely to be destructive in nature. The impetus for this is renewed Russian and Chinese space and counterspace developments and the recent conclusion that the United States is engaged in great power competition with Russia and China. The United States has also undertaken a major reorganization of its military space capabilities by creating a separate military service, the US Space Force, and combatant command, US Space Command, dedicated to space.

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

1.1 — US CO-ORBITAL ASAT

Assessment /
The United States has conducted multiple tests of technologies for close approach and rendezvous in both LEO and GEO, along with tracking, targeting, and hit-to-kill (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 offensive 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 never had an operational co-orbital ASAT program during the Cold War, it has had proposals for such a program and did test and develop many of the underlying technologies. Most notably, several of the technologies for space-based ballistic missile intercept developed as part of 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 initially as a satellite inspector but could be turned into a co-orbital ASAT weapon. The concept began because of a set of studies done from 1956 through 1959 on ways to defend against hostile satellites.[1] 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 concerns about an unidentified space object that was detected in December 1959 (that later turned out to be a piece of debris from the US Discoverer V satellite).[2]

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 onboard television cameras and radars to inspect the target from as close as 50 feet. However, the USAF also hoped that a 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 for SAINT to be fully operational by the summer of 1967.[3] However, lack of budget support and political concerns led to the program's cancellation in 1962, before any on-orbit tests were conducted.

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 SDI. The goal of the Delta 180 experiment was to better understand tracking, guidance, and control for a space intercept of an accelerating target.[4] The experiment involved modifying the second stage of a Delta 2 rocket (D2) to carry a sophisticated tracking system that included laser ranging, 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.[5] Sixteen pieces of orbital debris from the collision were cataloged with apogees as high as 2,300 km. Due to the low altitude of the intercept, most of the pieces reentered the atmosphere within two months. The final piece of debris reentered on April 4, 1987, more than seven months after the test.

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

2 Ibid, p. 112-113.

3 Ibid, p. 115.

4 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.

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

Recent US LEO RPO Activities

Since the end of the Cold War, the USAF, National Aeronautics and Space Administration (NASA), Defense Advanced Research Projects Agency (DARPA), and other US government agencies 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 US 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.[6] 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]."[7] The fact sheet also stated that over the following 12 to 18 months, the spacecraft "conduct[ed] rendezvous and proximity maneuvers with several US owned, dead or inactive resident space objects near its orbit." However, it is impossible to verify whether these activities occurred and whether XSS-11 visited any non-US space objects because the US military did not publish any positional information for the XSS-11 while in orbit.

FIGURE 1-1 — MINOTAUR UPPER STAGE

The image was taken by XSS-11 from a distance of approximately 500 m. Image credit: AFRL.[8]

On April 15, 2005, NASA launched the DART satellite (2005-014A, 28642) to conduct an autonomous rendezvous experiment with a US 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.[9]

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

6 Thomas M. Davis and David Melanson, "XSS-10 Micro-Satellite Flight Demonstration," Paper No. GT-SSEC.D.3: p.7. https://smartech.gatech.edu/bitstream/handle/1853/8036/SSEC_SD3_doc.pdf;jsessionid=906BB-52FE69F848048883B704DB20F07.smart2?sequence=2.

7 "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.

8 Ibid, p.2.

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

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.[10] The two spacecraft were deactivated in July 2007.[11]

FIGURE 1-2 — ORBITAL EXPRESS MISSION PLAN

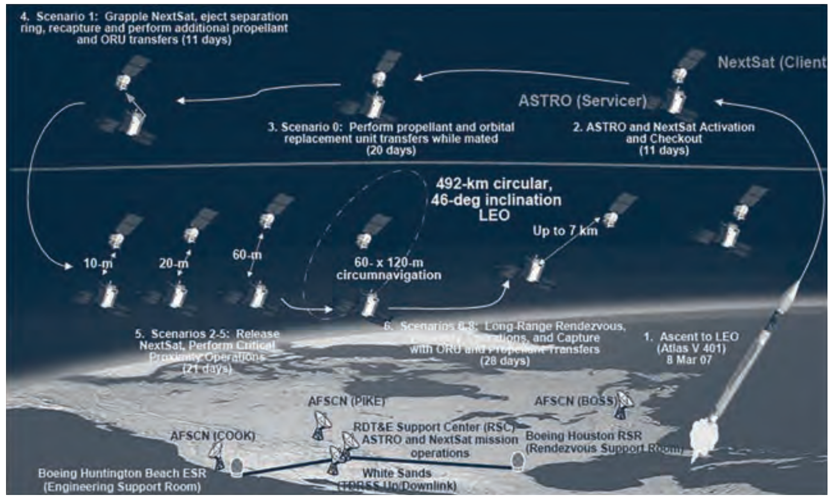


Image credit: Boeing.[12]

X-37B Robotic Spaceplane

The X-37B is a reusable robotic spacecraft that serves as a technology demonstrator and experimental vehicle. It is launched into orbit on a SLV, can stay in orbit for an extended period of time, and then glide to a runway landing.[13] The original X-37A was developed by NASA and derived from Space Shuttle concepts before transfer to DARPA in 2004. In 2006, the USAF took over the program and developed a new version, the X-37B, and produced two spacecraft known as Orbital Test Vehicles (OTVs) that have since flown seven missions, likely for testing new reusable space launch vehicle technologies (such as guidance and thermal protection) and on-orbit testing of new sensor technologies and satellite hardware for risk reduction.

On October 27, 2019, the OTV-5 flight of the X-37B completed an at that time 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.[14] Although a similar reference was made during the launch of OTV-5 in September 2017, it was perceived at that time to be 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 nor cataloged by the US 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 US military 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.[15]

10 "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.

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

12 "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/.

13 Stephen Clark, "Air Force spaceplane is an odd bird with a twisted past," Spaceflight Now, April 2, 2010, https://www.spaceflightnow.com/atlas/av012/100402x37update/.

14 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/.

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

The next 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 which was a satellite, FalconSAT 8, built by students at the USAF Academy, and was deployed in October 2021.[16] OTV-6 released another subsatellite at the end of May 2020, which was cataloged by the US military as USA 300 (2020-029B, 45610) indicating it was another separate payload.[17] OTV-6 also tested an on-orbit power beaming system, the US Naval Research Laboratory (NRL)'s Photovoltaic Radio-frequency Antenna Module (PRAM), that collected solar power and transformed it into a microwave beam. This was the first test of such capabilities in space and could eventually lead to large-scale space-based solar power, but could also provide offensive DEW counterspace capabilities.[18] OTV-6 also carried NASA payloads that did not separate, including Materials Exposure and Technology Innovation in Space (METIS-2), which tested candidate radiation shielding materials, printed electronic materials, and thermal control coatings; METIS-1 had been on OTV-5.[19] Boeing and SpaceX later released a video showing the X-37B and its payload module separating from the launch rocket.[20] Russian reports claimed that the X-37B released a small object in October 2021, which spent a day keeping about 200 meters away from the object, and then moved away from it.[21] The US military's public satellite catalog lists an additional object associated with the launch as USA 299 DEB (54246, 2020-029D) but has not provided orbital data for any objects associated with OTV-6 before it returned to Earth.

OTV-6 landed in November 2022 after spending 908 days in orbit, which was a new record for the X-37B.[22] The service module separated from the plane prior to landing and is thought to have burned up in the Earth's atmosphere during reentry; Secretary of Air Force Frank Kendall pointedly stated, "The deliberate manner in which we conduct on-orbit operations to include the service module disposal speaks to the United States' commitment to safe and responsible space practices, particularly as the issue of growing orbital debris threatens to impact global space operations."[23]

The most recent X-37B mission is OTV-7 (USA 349, 2023-210A, 58666), which was launched in December 2023 after being delayed twice, first due to weather, and then second because of ground equipment issues.[24] USSF officials said prior to the launch that tests of the X-37B would include "operating the reusable spaceplane in new orbital regimes, experimenting with future space domain awareness technologies, and investigating the radiation effects on materials provided by NASA."[25] It was spotted by an amateur astronomer in February 2024 in a HEO of 323 x 38,838 km x 59.1 deg inclination,[26] which is significantly higher than earlier test flights (which stayed well within LEO) and also distinct from other well-known HEO missions, such as the Soviet/Russian Molniya satellites.

16 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/.

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

18 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.

19 Thomas Newdick, "Details About X-37B Payload Adapter Revealed After Record-Setting Mission," The War Zone, November 14, 2022, https://www.thedrive.com/*the-war-zone*/details-about-x-37b-payload-adapter-revealed-after-record-setting-mission.

20 Joseph Trevithick, "Look At An X-37B In Space With An Extended Payload Module," *The War Zone*, December 29, 2023, https://www.twz.com/this-appears-to-be-our-first-look-at-an-x-37b-in-space.

21 Dmitry Stefanovich, Twitter, December 8, 2021, https://twitter.com/KomissarWhipla/status/1468593293235793924?s=20; Vladimir Kozin, "Cold Star War: The US has Questions for Moscow about Space, Russia has even more Questions for the US," *VKP-News*, November 29, 2021, https://vpk-news.ru/articles/64859.

22 Stefano D'Urso and David Cenciotti, "Reflecting On The X-37B's Latest Record-Breaking Mission," *The Aviationist*, *December 24, 2022*, https://theaviationist.com/2022/12/24/reflecting-on-the-x-37bs-latest-record-breaking-mission/.

23 Newdick, ibid.

24 Mike Wall, "SpaceX Falcon Heavy rocket launches mysterious X-37B space plane for US Space Force after delays," Space.com, December 28, 2023, https://www.space.com/spacex-falcon-heavy-x-37b-space-plane-launch-success.

25 "Department of the Air Force scheduled to launch seventh X-37B mission," *Air Force News Service*, November 8, 2023, https://www.spaceforce.mil/News/Article-Display/Article/3583347/department-of-the-air-force-scheduled-to-launch-seventh-x-37b-mission/.

26 Jonathan McDowell, "Congrats to Tomi Simola for locating the secret X-37B spaceplane. OTV 7 is in a 323 x 38838 km x 59.1 deg orbit. Could be testing out a new HEO IR sensor for future early warning satellites - just a wild speculation on my part here.", Posted on Twitter, February 9, 2024, https://twitter.com/planet4589/status/1755974823119872007?s=20.

FIGURE 1-3 — X-37B OTV 7 HIGHLY ELLIPTICAL ORBIT

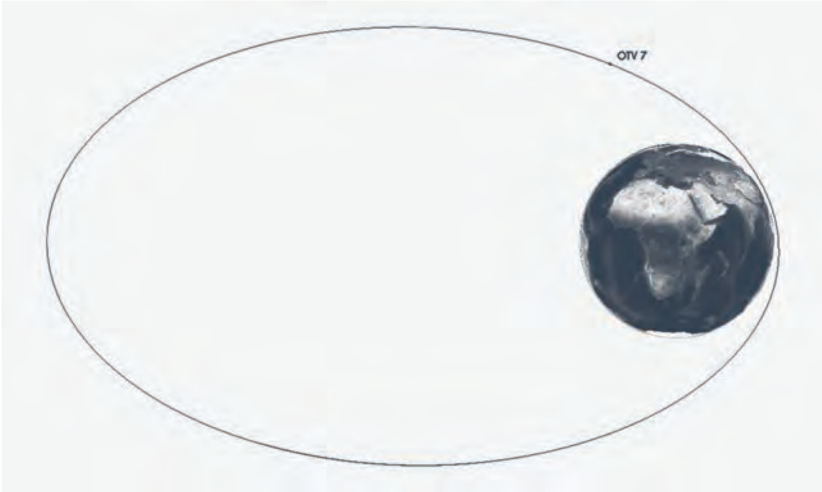


Image credit: Marco Langbroek.[27]

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.[28] However, the secrecy has led to a huge amount of speculation, particularly by Russia and China, that the X-37B is some sort of orbital bomber or secret weapons testing platform. Not helping calm concerns about its mission was the release of the USSF's first official painting in October 2023, which showed a military space plane described only as a "futuristic intercept vehicle" getting ready to engage with an enemy satellite; the USSF stated that they had the artist "rely on historic space planes and his own imagination" for the painting.[29] 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 "conducts protect and defend operations from space and provides response options to deter and defeat adversary threats in space."[30]

Analyzing the known facts about the size, shape, and orbit of the X-37B provides a more useful answer. The spaceplane resembles the now-retired space shuttle orbiter in overall shape but is much smaller, completely robotic, and as initially designed, has a payload bay that is roughly the size of a pickup truck bed.[31] The ring-shaped service module added for OTV-6 does increase what it can carry. However, it still has a limited ability to host weapons, and its limited gliding capability and maneuverability makes it not militarily useful as an orbital bomber.[32] Based on tracking data from hobbyists, the X-37B historically 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. Given the most recent OTV-7 mission is in a much higher altitude of nearly 39,000 km, it is possible it is testing out a new type of sensor or payload, but it is unclear what kind or why. While it likely has substantive maneuvering capability, to date, the X-37B has not approached nor 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

27 Marco Langbroek, "Imaging the X-37B robotic spaceplane mission OTV-7," *SatTrackCam Leiden (b)log*, February 13, 2024, https://sattrackcam.blogspot.com/2024/02/imaging-x-37b-robotic-spaceplane.html.

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

29 Brett Tingley, "US Space Force's 1st official painting shows military space plane intercepting adversary satellite," Space.com, October 24, 2023, https://www.space.com/space-force-painting-plane-intercepting-satellite.

30 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.

31 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.

32 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.

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 US military and intelligence satellites—calls into question the trustworthiness of the public SSA data provided by the US military. However, similar behavior in terms of secret deployments has also been seen by the Chinese Shenlong spaceplane (see Chinese Co-Orbital ASAT, Section 3.1).

Recent US 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,[33] and matched the description given in a 2004 NBC news article about a classified US government satellite program that had run afoul of Congress.[34] 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 US space missions.[35] Observers speculated that the MiTEx satellites would be conducting RPO in GSO.[36] In 2009, news reports revealed that they had been used to conduct "flybys" of the US early-warning satellite DSP 23, which had mysteriously failed on orbit shortly after launch.[37] Observations from hobbyists noted that the two MiTEx satellites 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.

A classified satellite publicly known only as PAN (USA 207, 2009-047A), was launched on September 8, 2009, into GEO orbit, where it was observed relocating every six months or so, until late 2013; its nine moves over four years placed it near several other satellites.[38] Then it stayed in a stable position until roughly February 2021, when it appears to have started moving again.[39] Amateur observers were able to observe it again starting in August 2023, station-keeping at 39.7 degrees East, so it is assumed that it is still active.[40] In September 2023, it was spotted drifting westward.[41] As of December 2023, it was seen very near the satellite EXPRESS AMU-1 but still drifting westward.[42] Very little is known about the mission of PAN, although most public observers believe it has a signals intelligence mission and could be conducting similar activities to the Russian Luch/Olymp-K satellite (see Russian Co-Orbital ASAT, Chapter 2.1).

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 (GSSAP), which may have the internal codename of Hornet. GSSAP consists of multiple pairs of small satellites deployed in near-GEO orbits, with altitudes slightly above or below the GSO belt, which allow them to drift east or west relative to other GSO satellites

33 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.

34 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/.

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

36 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.

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

38 Marco Langbroek, "A NEMESIS in the Sky: PAN, MENTOR 4, and Close Encounters of the SIGINT Kind," *TheSpaceReview.com*, October 31, 2016, https://www.thespacereview.com/article/3095/1.

39 Marco Langbroek, "PAN (NEMESIS 1) is on the Move Again," *SatTrackCam Leiden Blog*, September 14, 2021, https://sattrackcam.blogspot.com/2021/09/pan-nemesis-1-is-on-move-again.html.

40 Marco Langbroek, "Recovering USA 310, PAN and Trumpet 2," *SatTrackCam Leiden Blog*, September 10, 2023, https://sattrackcam.blogspot.com/2023/09/recovering-usa-310-pan-and-trumpet-2.html.

41 Marco Langbroek, "PAN is on the move again," *SatTrackCam Leiden Blog*, September 16, 2023 https://sattrackcam.blogspot.com/2023/09/pan-is-on-move-again.html.

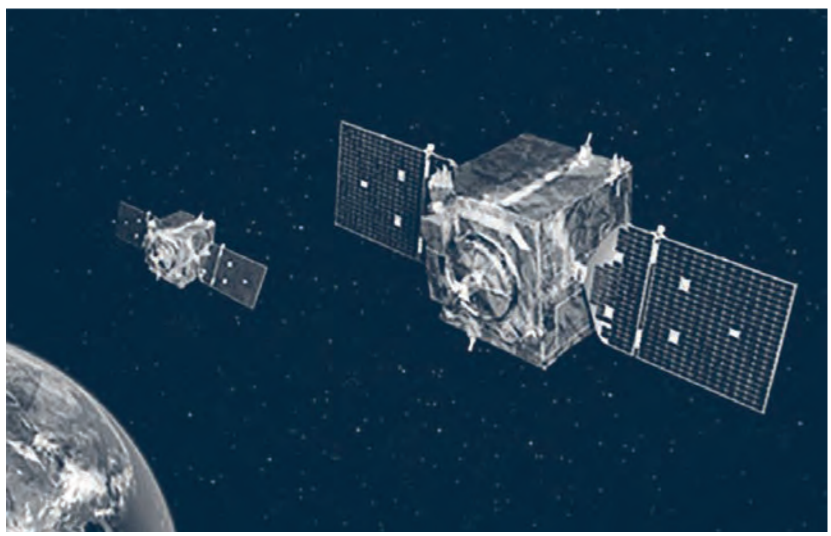
42 Marco Langbroek, Posted on Twitter, December 19, 2023, https://twitter.com/Marco_Langbroek/status/1737239557010018748?s=20.

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

and provide close inspections of objects in the GEO region.[43] The official USAF fact sheet states that the GSSAP satellites can conduct RPO of "resident space objects of interest."[44] The first pair of GSSAP satellites (USA 253, 2014-043A; USA 254, 2014-043B) was 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. A third pair (USA 324, 2022-006A, 51280; USA 325, 2022-006B, 51281), was launched in January 2022.[45] The US Space Systems Command confirmed in August 2023 that one of the satellites from the pair launched in 2014, GSSAP Space Vehicle (SV) 2, had reached its end of life and been placed in a graveyard orbit.[46] Two more launches of new GSSAP satellites are planned to occur in 2024 and 2027.[47] Very limited public information is known about the on-orbit activities of the five remaining GSSAP satellites, as the USAF does not disclose information on their orbits; they are thought to operate in pairs, with one satellite staying below the GEO belt, and one operating above it.[48] The GSSAP satellites are operated by the 1st Space Operations Squadron of the USSF's Space Delta 9, which has a mission to conduct orbital warfare.[49]

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.[50] According to General Hyten, the two satellites provided what he deemed "eye-watering" pictures of one or more objects in GSO.

FIGURE 1-4 — GSSAP SATELLITES



Artist's depiction. Image credit: US Air Force.[51]

Although the US 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 1-1. The GSSAP satellites have done close approaches of several US military satellites, several Russian and Chinese military satellites, and commercial satellites built by China and operated by other countries. According to Russian sources, some of these close approaches involved the GSSAP satellite making many small phasing

43 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.

44 "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/.

45 "GSSAP 1, 2, 3, 4, 5, 6," Gunter's Space Page, accessed March 22, 2018, http://space.skyrocket.de/doc_sdat/gssap-1.htm; Theresa Hitchens, "Space Force to loft 2 new 'neighborhood watch' sats, as leader frets launch funds," *BreakingDefense*, January 21, 2022, https://breakingdefense.com/2022/01/space-force-to-loft-2-new-neighborhood-watch-sats-as-leader-frets-launch-funds/.

46 Sandra Erwin, "U.S. deactivates GSSAP surveillance satellite, two new ones in the works," *SpaceNews*, August 15, 2023, https://spacenews.com/u-s-deorbits-gssap-surveillance-satellite-two-new-ones-in-the-works/.

47 Hillary Gibson, "Mission Complete: GSSAP SV2 transfers to SSC," Space Operations Command, August 2, 2023, https://www.spaceforce.mil/News/Article-Display/Article/3486658/mission-complete-gssap-sv2-transfers-to-ssc/.

48 Mariia Kiseleva, "USSF-8 / Atlas V 511," *EverydayAstronaut*, January 13, 2022, https://everydayastronaut.com/ussf-8-atlas-v-511/.

49 Joseph Trevithick, "Space Force Has A Unit Dedicated To Orbital Warfare That Now Operates The X-37B Spaceplane," The War Zone, 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.

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

51 "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/.

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 14 one- and two-impulse maneuvers during their proximity operations of WGS 4 (2012-003A, 38070), a US military communications satellite, which raised concerns about whether it was testing co-orbital technologies. The US military began releasing public positional information for the four GSSAP satellites active at the end of 2019, although some of the data are weeks or months old.

TABLE 1-1 — SATELLITES APPROACHED BY GSSAP THROUGH JANUARY 2022[52]

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
Aug. 23, 2020	SJ-20/Chinasat 6A	China	24 km
Jan. 2022	SY-12 01, SY-12 02	China	73 km

In a video released by the commercial SSA company COMSPOC, it can be seen that USA 271 approached China's SJ-20 satellite in August 2020, getting within 20 km of it.[53] In late January 2022, one of the four GSSAP satellites, USA 270, maneuvered to approach a pair of Chinese satellites, SY-12 (01) (2021-129A, 50321) and SY-12 (02) (2021-129B, 50322), that had recently been launched into GEO (see Chinese Co-Orbital ASAT, Section 3.1). According to tracking data collected by ExoAnalytic Solutions, SY-12 01 and SY-12 02 made significant maneuvers to split up and begin rotating around the GEO belt in opposite directions, with SY-12 02 apparently also getting an imaging opportunity on USA 270.[54] A video animation released by COMSPOC Corporation also shows the encounter.[55]

A Chinese paper released in 2023 indicated that they had tracked GSSAP satellites conducting at least 14 uncoordinated close approaches with six Chinese satellites (Tianlian 2-01, BD-2 G8, SJ-20, TJS-2, TJS-3, and TJS-5) in 2020 and 2021.[56]

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.[57] The goal of ANGELS was to provide a clearer picture of the local area around important US national security satellites in GSO. The 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

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

53 Colin Clark, "US, China, Russia Test New Space War Tactics: Sats Buzzing, Spoofing, Spying," BreakingDefense, October 28, 2021, https://breakingdefense.com/2021/10/us-china-russia-test-new-space-war-tactics-sats-buzzing-spoofing-spying/.

54 Debra Werner, "An In-Orbit Game of Cat and Mouse: Close approaches prompt calls for communications and norms," *SpaceNews*, June 16, 2022, https://spacenews.com/an-in-orbit-game-of-cat-and-mouse-close-approaches-prompt-calls-for-communications-and-norms/.

55 SpaceNewsInc,"USA 270/Shiyan12 encounter," Youtube, Accessed February 22, 2023, https://www.youtube.com/watch?v=H0ZlgmdjXjw.

56 Stephen Chen, "Study says US spy satellites approaching China's high-value space assets a 'threat to security'," *South China Morning Post*, May 5, 2023, https://www.scmp.com/news/china/science/article/3219350/too-often-too-close-study-says-us-spy-satellites-approaching-chinas-high-value-space-assets-threat.

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

upper stage and conducted a series of RPO maneuvers to close within a few kilometers.[58] 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 entirely inert. The USAF originally did not disclose orbital information for either ANGELS or the Delta 4 upper stage but began to do so in February 2020. ANGELS was decommissioned in November 2017 and remains in a GEO graveyard orbit.[59]

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.[60] 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.[61]

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), 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."[62] The US military has not provided any information on the other two payloads. In January 2020, the US military began providing public orbital information for CBAS, the Centaur upper stage, and the other two unnamed payloads, but not EAGLE or Mycroft.[63]

In October 2019, the USAF announced that Mycroft was being sent to inspect another US satellite in the GEO region, S5 (2019-009D, 44065).[64] 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.[65] The USAF stated that Mycroft would conduct a series of RPO maneuvers with S5 over a period of weeks to try and determine the 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.[66]

TABLE 1-2 — RECENT US RPOs

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 US space objects in nearby LEO orbits over the next 12-18 months.
Apr. 2005	DART, MUBLCOM	LEO	DART did a series of autonomous maneuvers to bring it close to the MUBLCOM satellite and ended up bumping into it.
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.

58 "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.

59 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/.

60 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/.

61 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.

62 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/.

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

64 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/.

65 Ibid.

66 Scott Tilley, Tweet, December 21, 2019, https://twitter.com/coastal8049/status/1208475681790627841?s=20.

DATE(S)	SYSTEM(S)	ORBITAL PARAMETERS	NOTES
Dec. 23, 2008 and Jan.1, 2009	DSP-23, MiTEx (USA 187, USA 188)	GEO	Inspection and close rendezvous with a failed US satellite. Possibly other demonstrations and tests in geosynchronous orbit.
2009 – 2013	Yahsat 1B, others unknown, PAN (USA-207)	GEO	Part of NRO's Nemesis satellites (geostationary COMINT).Presumed to have completed SIGNIT (signals intelligence) with other satellites. Unique for roaming various times to different orbits and satellites.
Jul. 2014 – present	GSSAP, multiple objects	GEO	Multiple 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.
Aug. 2020	SJ-20, USA 271	GEO	In August 2020, USA 271 approached China's SJ-20, shadowing the spacecraft. The Chinese spacecraft detected the US satellite and rapidly moved away.
Jan. 2022	Shiyan-12(01) and Shiyan-12(02), USA 270	GEO	In January 2022, USA 270 approached China's Shiyan-12(01) and (02) satellites in GEO. As USA 270 approached, the Shiyan-12 satellites maneuvered away to drift orbits. The closest approach was around 73 kilometers.

In April 2023, USSF Space Systems Command (SSC) launched small satellite known as Tetra-1 (USA 340, 2022-144E, 55138) into an orbit at around 38,000 kilometers altitude, which is well above the active GEO belt.[67] The Tetra-1 small satellite is intended to practice maneuvering and other activities needed to survive an altitude that is often used as a graveyard orbit for satellites at GEO.[68] SSC used Tetra-1 in a series of training maneuvers with Space Delta 11 as part of an exercise referred to as "Scarlet Star."[69] It is unknown if Tetra will be doing any RPO or conducting any SSA activities.

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 relatively slow and methodical approaches to rendezvous with other space objects in similar orbits. The satellites they are known to have approached were in similar orbits and, based on the publicly available data, they did not make huge changes to rendezvous with satellites in significantly different orbits. This behavior is similar to several international RPO missions to test and demonstrate satellite inspection and servicing capabilities, in particular the Chinese SJ-12, SJ-15, SJ-17, and TJS-3 satellites (see Chinese Co-Orbital ASAT, Section 3.1) 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, particularly 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.

67 Debra Werner, "Space Systems Command's Tetra-1 begins mission operations," *SpaceNews*, April 13, 2023, https://spacenews.com/tetra-1-begins-mission-operations/.

68 Werner, "Space Systems Command's," April 13, 2023, ibid.

69 Werner, "Space Systems Command's," April 13, 2023, ibid.

1.2 — US 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 a low LEO satellite. 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 US 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
US 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 United States 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.[70] These tests led to the development of the first DA-ASAT program built from the Nike Zeus anti-ballistic missile.

NOTSNIK, HiHo, and Satellite Interceptor Program (SIP)
During the 1960s, the US 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. In 1958, the Navy started working on a program (known as Project Pilot or, more commonly, NOTSNIK) that would give the United States an air-launched SLV capability; after 10 launch failures, NOTSNIK was halted, with efforts focusing on an improved launch vehicle, the Caleb rocket, also known as NOTS-EV-2.[71] In 1962, the Navy began work on Project HiHo, which involved a Caleb rocket fired from a Phantom 4D fighter bomber aircraft.[72] Although the primary focus was on developing an air-launched SLV, a secondary objective was to develop ASAT capabilities. Three test launches in space were conducted from 1961 to 1962; the first two failed but the third reached an apogee of 1,600 km. In the end, the Navy decided not to pursue an operational version.[73] Subsequently, the Navy investigated using the NOTS-EV-2 launch vehicle but adapted for ground-launch as part of a program known as the Satellite Interceptor Program (SIP). There were two launches (held in October 1961 and May 1962) that apparently were successful tests, but little else is known about them.[74]

70 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.

71 Gunter D. Krebs, "Pilot (NOTS-EV-1, NOTSNIK)," *Gunter's Space Page*; accessed February 21, 2022, https://space.skyrocket.de/doc_lau/nots1.htm.

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

73 Gunter D. Krebs, "Caleb (NOTS-EV- 2)," *Gunter's Space Page*, accessed February 20, 2022, https://space.skyrocket.de/doc_lau/caleb.htm.

74 Jeff Scott, "NOTSNIK, Project Pilot & Project Caleb," April 23, 2006, http://www.aerospaceweb.org/question/spacecraft/q0271.shtml. Accessed February 20, 2022.

FIGURE 1-5 — SATELLITE INTERCEPTOR PROGRAM GROUND TEST

Image credit: Aerospaceweb.org

Nike Zeus

The Nike Zeus ASAT Program was developed out of anti-ballistic missile testing of the US Army's Nike Zeus system and later came to be known as Program 505. Beginning in 1957, the US Army argued that its Nike Zeus ABM system could have an ASAT capability added to it to help defend against ICBMs and space threats.[75] 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 an 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.[76] Testing continued throughout the early 1960s but eventually

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

76 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.

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

gave way to Program 437, which demonstrated greater performance and would extend through the remainder of the decade.

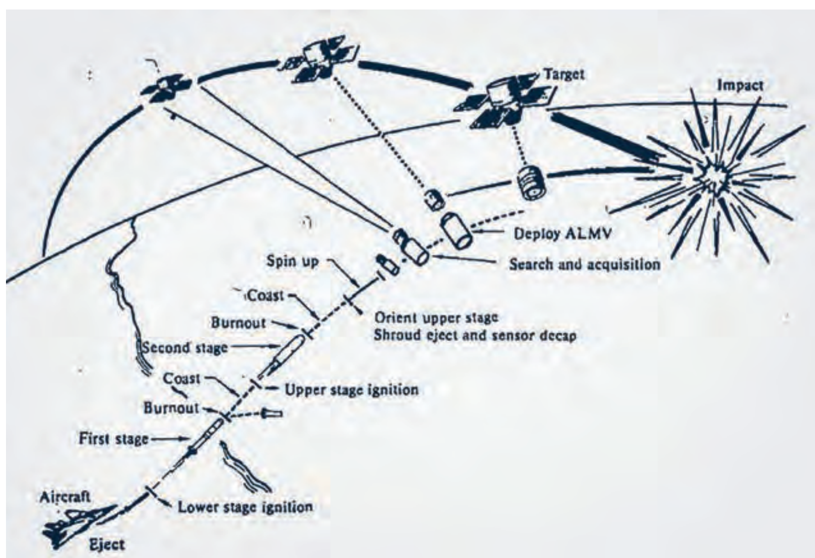
Program 437

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.[77] 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 8 kilometers.[78] The missiles and warheads were stored at Vandenberg AFB in California, while the Thors were operated out of Johnston Atoll, so they required a two-week notification to get the missiles and warheads to their launch vehicle.[79] On August 6, 1963, President Kennedy directed that Program 437 be given the highest national priority category for further research and development.[80] 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.[81]

ASM-135 Air-Launched DA-ASAT

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.[82] 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.[83] Five flight tests occurred,[84] 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 US missile destroyed a satellite prior to 2008.[85]

FIGURE 1-6 — ASM-135 FLIGHT PROFILE[86]



Credit: US Department of Defense.

The ASM-135 had an estimated operational range of 648 km, flight ceiling of 563 km, and speed of over 24,000 km/h.[87] 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

77 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/_/cMg-dYypcPc8C?hl=en&gbpv=1&pg=PP1.

78 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.

79 Mark Wade, "Program 437," *Astronautix.com*, http://www.astronautix.com/p/program437.html, accessed Feburary 19, 2021.

80 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.

81 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.

82 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.

83 Ibid.

84 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.

85 "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/.

86 *Soviet Satellite Defense Against the US Miniature Vehicle Antisatellite Weapon (U): An Intelligence Assessment*, Office of Scientific and Weapons Research, Central Intelligence Agency, SW83-10062, September 1983, https://www.archives.gov/files/declassification/iscap/pdf/2012-151-doc01-03.pdf.

87 Parsch, "Vought ASM-135 ASAT."

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.[88] A CIA document from 1983 about the system (calling it then the Air-Launched Miniature Vehicle program, or ALMV) noted how various Soviet satellite systems would fare against the system; included in thegroup was the crewed Salyut Soviet space station.[89] This was likely due to some of the Salyuts actually being secret Soviet Almaz military space stations (see Russian Co-orbital ASAT, Section 2.2).

The USAF had planned to deploy an operational force of 112 ASM-135 missiles, to be deployed aboard 20 modified F-15s.[90] Fifteen 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.

TABLE 1-3 — HISTORY OF US DA-ASAT TESTING

DATE	ASAT SYSTEM	SITE	TARGET	APOGEE	NOTES
Sept. 22, 1959	High Virgo (TX-20)	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)
Oct. 1, 1961	SIP (NOTS-EV-2)	San Nicolas Island	None	Unknown	Successful rocket test
Oct. 5, 1961	HiHo (NOTS-EV-1)	F4D-I	None	Unknown	Rocket failure
Mar. 26, 1962	HiHo (NOTS-EV-1)	F4D-I	None	Unknown	Rocket failure
May 5, 1962	SIP (NOTS-EV-2)	F4-C	None	Unknown	Successful rocket test
Aug. 26, 1962	HiHo (NOTS-EV-1)	F4-C	None	1,600 km	Successful rocket test
Dec. 17, 1962	Program 505 (Nike Zeus)	WSMR	None	160 km	Success (reached designated point in space)
Feb. 15, 1963	Program 505 (Nike Zeus)	Kwajalein	None	241 km	Successful intercept of designated point in space
Mar. 21, 1963	Program 505 (Nike Zeus)	Kwajalein	None	–	Unsuccessful attempt to intercept simulated satellite target
Apr. 19, 1963	Program 505 (Nike Zeus)	Kwajalein	None	–	Unsuccessful attempt to intercept simulated satellite target
May 24, 1963	Program 505 (Nike Zeus)	Kwajalein	Agena D	Unknown	Successful close intercept
Jan. 4, 1964	Program 505 (Nike Zeus)	Kwajalein	None	146 km	Successful intercept of a simulated satellite target
Feb. 14, 1964	Program 437 (Thor)	Johnston Atoll	Transit 2A Rocket Body	1000 km	Success (passed within kill radius)
Mar. 1, 1964	Program 437 (Thor)	Johnston Atoll	Unknown	674 km	Success (primary missile scrubbed, backup missile passed within kill radius)
Apr. 21, 1964	Program 437 (Thor)	Johnston Atoll	Unknown	778 km	Success (passed within kill radius)
May 28, 1964	Program 437 (Thor)	Johnston Atoll	Unknown	932 km	Failed (missed intercept point)

88 "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.

89 *Soviet Satellite Defense Against the US Miniature Vehicle Antisatellite Weapon (U): An Intelligence Assessment*, Office of Scientific and Weapons Research, Central Intelligence Agency, SW83-10062, September 1983, https://www.archives.gov/files/declassification/iscap/pdf/2012-151-doc01-03.pdf.

90 Parsch, "Vought ASM-135 ASAT."

DATE	ASAT SYSTEM	SITE	TARGET	APOGEE	NOTES
Nov. 16, 1964	Program 437 (Thor)	Johnston Atoll	Unknown	1,148 km	Successful Combat Test Launch (passed within kill radius)
Mar. 1965	Program 505 (Nike Zeus)	Kwajalein	None	–	–
Apr. 5, 1965	Program 437 (Thor)	Johnston Atoll	Transit 2A Rocket Body	826 km	Successful Combat Test Launch (passed within kill radius)
June-July 1965	Program 505 (Nike Zeus)	Kwajalein	None	Unknown	Four test intercepts, of which three were successful
Jan. 13, 1966	Program 505 (Nike Zeus)	Kwajalein	None	Unknown	Successful intercept with simulated target
Mar. 30, 1967	Program 437 (Thor)	Johnston Atoll	Unknown piece of space debris	484 km	Successful Combat Evaluation Launch (passed within kill radius)
May 15, 1968	Program 437 (Thor)	Johnston Atoll	Unknown	823 km	Successful Combat Evaluation Launch (passed within kill radius)
Nov. 21, 1968	Program 437 (Thor)	Johnston Atoll	Unknown	1,158 km	Successful Combat Evaluation Launch (passed within kill radius)
Mar. 28, 1970	Program 437 (Thor)	Johnston Atoll	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, debris created
Aug. 22, 1986	ASM-135	Aircraft	Star	1,000 km	Successful test in tracking
Sept. 5, 1986	Delta 180 Payload Adapter System	AFETR	Delta 2/B	326 km?	Successful intercept of thrusting object in 220-km circular orbit, debris created
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

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16

two, only the SM-3 has been demonstrated in a DA-ASAT role. In 2008, the US Operation Burnt Frost used an SM-3 Block IA interceptor fired from an Aegis Cruiser to destroy an ailing US reconnaissance satellite at an altitude of 240 km.[91] 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 (see Imagery Appendix, pg. 16-01), and Vandenberg Air Force Base, California,[92] with plans underway to deploy an additional 20 interceptors.[93] The planned burnout speed of the GBIs is reported to be 7 to 8 km/s.[94] 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 LEO, 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 in 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 to attack.

The current SM-3 Block IA and IB interceptors are less capable as DA-ASATs than the current GBIs - they can only reach the relatively few satellites in orbits with perigees at or below 600 km altitude.[95] However, the SM-3 Block IIA interceptors, currently under joint development with Japan, are intended to defend larger areas against more capable threats; even using a conservative estimate of the burnout speed for such a missile (4.5 km/s), it would be able to reach the vast majority of LEO satellites as shown in Table 1-4. 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 1-4 — MAXIMUM ALTITUDE REACHABLE BY SM-3 VARIANTS[96]

SM-3 VARIANT	BURNOUT VELOCITY (KM/S)	MAXIMUM REACHABLE ALTITUDE (KM)
Block IA	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 US 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.[97] was delayed for years due to construction issues but was finally accepted by the US Navy in December 2023; the US Navy then almost immediately started working on upgrades in preparation for transferring it over to NATO's command and control, something that is planned to happen mid-year 2024.[98] At one point, Japan was planning on joining the Aegis Ashore program, but canceled construction in

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

92 Kelley M. Sayler, Coordinator, CRS In Focus IF10541, *Defense Primer: Ballistic Missile Defense*, Congressional Research Service, updated January 30, 2024, https://sgp.fas.org/crs/natsec/IF10541.pdf. Originally authored by Stephen M. McCall, former Analyst in Military Space, Missile Defense, and Defense Innovation.

93 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/.

94 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.

95 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.

96 Ibid, p. 76.

97 Sam LaGrone, "Aegis Ashore Site in Romania Declared Operational," *USNI News*, May 12, 2016, https://news.usniorg/2016/05/12/aegis-ashore-site-in-romania-declared-operational.

98 Jen Judson, "Aegis Ashore Poland enters maintenance period ahead of NATO acceptance," Defense News, January 22, 2024, https://www.defensenews.com/naval/2024/01/22/aegis-ashore-poland-enters-maintenance-period-ahead-of-nato-acceptance/; John Vandiver, "European missile defense nears integration of US Aegis Ashore system in Poland," Stars and Stripes, December 21, 2023, https://www.stripes.com/branches/navy/2023-12-21/navy-poland-missile-defense-12427699.html.

June 2020.[99] The number of ballistic missile defense (BMD)-capable Aegis ships is expected to go from 43 to 56 (end of FY2025) [100] 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 rapid development of space-based reconnaissance capabilities to target anti-ship ballistic missiles against US ships.[101] 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.[102]

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 LEO 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 the range of fixed interceptor sites. This positioning flexibility also means that the SM-3 missiles would not have to expend much of their thrust going cross-range and could retain the ability to reach the highest LEO satellites. The more powerful GMD interceptors also could use some of their fuel to reach out laterally over thousands of kilometers, allowing them to hit satellites in orbits that do not pass directly over the GMD missile fields in Alaska, and California.

1.3 — US ELECTRONIC WARFARE

Assessment /
The United States has an operational EW counterspace system, the Counter Communications System (CCS), which can be deployed globally to provide uplink jamming capability against geostationary communications satellites. It is working on Meadowlands, an updated version of the CCS system.

Through its Navigation Warfare program, the United States has the capability to jam and interfere with the civil signals of global navigation satellite services (GNSS) 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 could jam military GNSS signals as well, although the effectiveness is difficult to assess based on publicly available information. The effectiveness of US measures to counter adversarial jamming and spoofing operations against military GPS signals is not known.

Specifics /
The following paragraphs provide a general overview of different types of EW capabilities as related to counterspace applications that are relevant 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." [103] 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." [104]

99 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/.

100 CRS In Focus IF10541, Defense Primer, ibid.

101 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.

102 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.

103 United States Department of Defense, "DOD Dictionary of Military and Associated Terms," Defense Technical Information Center, February 2018, p. 78, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

104 Ibid, p. 76.

In the case of satellite signals, jamming is often characterized as being either uplink or downlink, as shown in Figure 1-7. 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 retransmitted by the satellite and received by the users on the ground consists of indecipherable noise. The impact may be widespread since all users within the satellite's service area (known as the footprint) are affected. Downlink, or terrestrial, jamming targets the ground user of satellite services, by broadcasting an 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 1-7 — UPLINK VS. DOWNLINK JAMMING

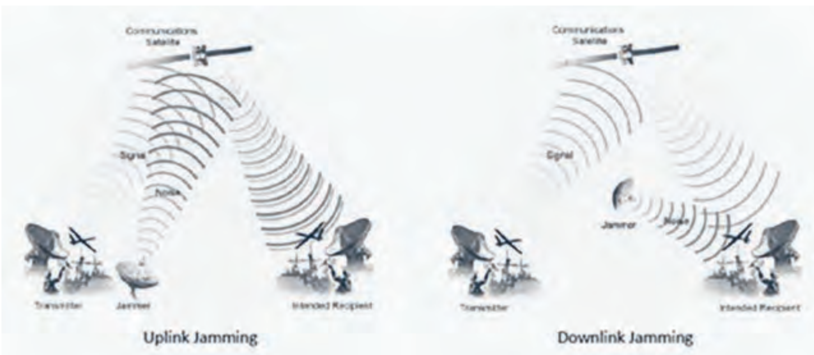


Image credit: Infosec Institute.[105]

A second type of EW attack is known as spoofing, which is altering the content of a signal or broadcasting a false signal in order to confuse or manipulate the end user. For example, an attacker might broadcast the same signal as a real one but at higher power in an attempt to get end users to use the spoofed signal instead of the real one, thereby allowing the attacker to use that spoofed signal to send their own information. In some cases, it is possible for an attacker to intercept and manipulate the real signal, enabling them to inject or alter the information that it carries.

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 or spoofing of:

1. GNSS signals,
2. Satellite communications, and
3. Synthetic aperture radar (SAR) imaging.

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

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

105 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.

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.[106]

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, and testing and procurement of a capability to provide jamming of satellite communications signals in response to USSTRATCOM requirements.

The limited 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 (March 2023), the description has evolved somewhat, offering more insight into the role of the CCS. It states that the "program provides expeditionary, deployable, reversible offensive space control (OSC) effects applicable across the full spectrum of conflict. It prevents adversary satellite communications (SATCOM) in the Area of Responsibility (AOR) including Command and Control (C2), Early Warning, and Propaganda; and hosts Rapid Reaction Capabilities in response to Urgent Needs."[107]

There is no public information on any technical characteristics 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, the CCS is likely targeted mainly at geostationary communications satellites (COMSATs), given that they are currently the primary source of satellite communications.

FIGURE 1-8 — SPACE FORCE GUARDIAN IN FRONT OF A PAIR OF COUNTER COMMUNICATIONS SYSTEM ANTENNAS

Image credit: L3Harris.[108]

106 "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/FY21/RDTE_/FY21%20Space%20Force%20Research%20Development%20Test%20and%20Evaluation.pdf?ver=2020-02-11-083608-887.

107 Air Force, Justification Book Volume 1, Procurement, Space Force RDT&E Budget Item Justification: FY 2024, "CTRSPC / Counterspace Systems," , Program Element: PE 1206421F ," March 2023, Vol. 1-7, https://www.saffm.hq.af.mil/Portals/84/documents/FY24/Procurement/FY24%20Space%20Force%20Procurement.pdf?ver=ewSd5VeJkGwWEzaSq_cd_Q%3D%3D.

108 "Counter Communications System," L3Harris, https://www.l3harris.com/all-capabilities/counter-communications-system.

The CCS is operated and maintained by the 4th Electromagnetic Warfare Squadron (formerly the 4th Space Control Squadron), attached to Space Delta 3 of the US Space Force located at Peterson SFB, Colorado. The CCS units can be deployed globally to conduct mobile and transportable space superiority operations in support of global and theater campaigns.[109] The CCS is also operated by the 114th Electromagnetic Warfare Squadron (of the Air National Guard), which supports the Space Force.[110]

The first two CCS units were reportedly delivered in 2004.[111] 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.[112] 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.[113] 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.[114]

In March 2017, Harris was awarded a contract to provide Block 10.2 upgrades for 13 existing antennas across the CCS.[115] In October 2021, L3Harris was awarded a $120.7 million-contract to provide upgraded units to Space Force bases in the United States and classified overseas locations, with L3Harris required to produce 16 units by 2025.[116] According to L3Harris, there are currently 16 transportable units operated by US Space Force and Air National Guard units.[117] 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.[118] It is being built by L3Harris and was supposed to deliver four systems by April 2023; the USSF intends to launch a competition for 28 more units.[119] However, the system is behind schedule with delivery by L3Harris not expected until late 2024.[120]

109 "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/.

110 Jacob Hancock, "Space Control Squadron Redesignated Electronic Warfare Squadron," National Guard, January 30, 2023, https://www.nationalguard.mil/News/Article/3281489/space-control-squadron-redesignated-electronic-warfare-squadron/.

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

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

113 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/.

114 "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/.

115 "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.

116 Sandra Erwin, "L3 Harris wins $120 million contract to upgrade Space Force electronic jammers," *SpaceNews*, October 22, 2021, https://spacenews.com/l3-harris-wins-120-million-contract-to-upgrade-space-force-electronic-jammers/.

117 "Counter Communications System," L3Harris, Copyright 2023, accessed February 15, 2024, https://www.l3harris.com/all-capabilities/counter-communications-system.

118 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.

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

120 Anthony Capaccio, "Portable US Weapon to Jam Chinese, Russian Satellites Is Running Two Years Late," Bloomberg, June 29, 2023, https://www.bloomberg.com/news/articles/2023-06-29/portable-us-weapon-to-jam-chinese-russian-satellites-is-running-two-years-late?srnd=premium-asia.

The CCS continues to be well funded with activities including upgrades to existing systems as well as procurement of new units. Although it appears to be shifting to maintenance mode as the planned budget drops significantly after FY 2024: $52.7 million was requested for procurement in FY 2024, but FY 2025-2028 anticipates $10 million total. Having said that, the budget documents indicate that through FY 2028, $232 million will have been spent on the program.[121] There is no public information on theater deployments by the CCS. In March 2022, when discussing Russia's attack on Ukraine, Eric Desautels, the acting deputy assistant secretary for emerging security challenges and defense policy in the Department of State's Bureau of Arms Control, Verification and Compliance, stated that "the United States has our own communications jammer known as the CCS system," and that, "We think that jamming is probably a normal part of conflict;" however, he did not say if the CCS has been sent to the region.[122] 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.[123] However, it is clear from the funding allocations that the CCS is a high-priority program and likely offers the US military a very effective SATCOM jamming capability. The CCS system continues to be evolved, presumably with increasing sophistication and capability.

Black Skies

The Space Force undertook the first iteration of an EW training event called "Black Skies" in September 2022.[124] This event was intended to allow Space Force personnel to practice jamming satellites, focusing on a commercial satellite target leased by the Space Force for this purpose. The second one was held in March 2023, with the third happening in September 2023. The third iteration, Black Skies 23-3, had the Combined Space Operations Center (CSpOC) coordinating live fire exercises (where operators sent signals from ground to space), as well as closed loop operations (where there was no impact to space assets); including other units, there were over 170 people participating.[125] This is part of a larger testing series planned by the Space Force. "Red Skies" was held in December 2023 that strove to make training scenarios more realistic through incorporating space weapons simulations and allowing the participation of more operators); a "Blue Skies" event is planned that will focus on cyber operators.[126] Major General Shawn Bratton, the head of Space Training and Readiness Command, has said that they are considering a fleet of "live" on-orbit satellites that the Space Force could practice on.[127] The USSF has a live ground-based EW range—the Space Test and Training Range—at Schriever Space Force Base in Colorado.[128]

NAVWAR

The United States DoD relies heavily on PNT capabilities, which are primarily provided by GPS satellites. Over the last two decades, the US 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 US 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 US military could conduct both defensive and offensive operations to protect US use of PNT capabilities while also interdicting or preventing adversary use of PNT capabilities.[129]

The Joint Navigation Warfare Center (JNWC) was established by the 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

121 Air Force, Justification Book Volume 1, Procurement, Space Force RDT&E Budget Item Justification: FY 20243, "CTRSPC / Counterspace Systems," 1 Space Force, Program Element: PE 1206421F ," March 2023, Vol. 1-7, https://www.saffm.hq.af.mil/Portals/84/documents/FY24/Procurement/FY24%20Space%20Force%20Procurement.pdf?ver=ewSd5VeJkGwWEzaSq_cd_Q%3D%3D.

122 Theresa Hitchens, "Satellite jamming 'normal' by militaries during conflict, not peacetime: State Dept. official," BreakingDefense, March 21, 2022, https://breakingdefense.com/2022/03/satellite-jamming-normal-by-militaries-during-conflict-not-peacetime-state-dept-official/.

123 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-communications-system-block-102-achieves-ioc-ready-for-the-warfighter/.

124 Courtney Albon, "Space Force refining range needs through 'Black Skies' training," Defense News, September 22, 2022, https://www.defensenews.com/space/2022/09/22/space-force-refining-range-needs-through-black-skies-training/.

125 Unshin Lee Harpley, "Space Force Conducts Its Biggest Electronic Warfare Exercise Ever," Air & Space Forces Magazine, October 6, 2023, https://www.airandspaceforces.com/space-force-biggest-electronic-warfare-exercise-ever/.

126 Greg Hadley, "Red Skies: Space Force Launches New Orbital Warfare Exercise," Air & Space Forces Magazine, January 8, 2024, https://www.airandspaceforces.com/red-skies-space-force-new-orbital-warfare-exercise/.

127 Albon, September 22, 2022, ibid.

128 Albon, June 15, 2022, ibid.

129 *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.

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 "[t]o 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." [130] Most of the US NAVWAR capabilities and activities are classified, and hence there is little publicly available information. However, the US 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 US military developed a new military signal, called M-code, which is much more secure than the older P(Y) military GPS signal. M-code operates at a higher power and a waveform that increases its resistance to jamming, and improved encryption protocols to protect against spoofing.

New generations of GPS satellites, starting with the first GPS Block IIR-M satellite (NAVSTAR 57, 2005-038A, 28874) launched on September 26, 2005, are able to broadcast M-code. There are currently 24 M-code capable GPS satellites, including the first of the new GPS Block IIIA satellites launched on December 23, 2018.[131] Deployment of the ground control system (known as OCX) and new end user receivers to fully implement and utilize M-code have run into significant delays and challenges; the Director of Operational Test & Evaluation reported in January 2024 that the delay extended the delivery of OCX until July 2025 and pointed out, "These delays increase risk that U.S. and allied warfighters will be unable to conduct successful operations in future contested environments due to the lack of access to modernized GPS position, navigation, and timing (PNT) information." [132] 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,[133] 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.[134]

There is no confirmed public information on the US military's technical capabilities for offensively jamming or spoofing adversary PNT capabilities. Nevertheless, the United States likely has very effective capabilities for jamming and spoofing of GNSS receivers, including GPS, GLONASS, and BeiDou. This assessment is based on the consistent high priority placed on the NAVWAR effort, the success of US EW systems in other domains of warfare, and the technical sophistication of the US 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.[115] It is rumored that the United States interfered with GPS in the East China Sea region in order to disrupt a Chinese missile drill held during a time of heightened relations in 1996.[136]

The US military is also 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.[137] In August 2018 and February 2019, a US Navy Carrier Strike Group also exercised wide-scale jamming of GPS across the southeastern coast of the United States.[138] Wide-scale jamming was exercised along the southeastern coast of the United States on August 30, 2019, September 5, 2019,[139] and January 16–24, 2020.[140] And additional GPS jamming was carried out as part of tests over South Carolina, California, and Alaska in March 2022.[141]

130 "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/.

131 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/.

132 "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; Theresa Hitchens, "Ground system for jam-resistant GPS delayed again to July 2025 at earliest, Pentagon tester says," Breaking Defense, February 2, 2024, https://breakingdefense.com/2024/02/ground-system-for-jam-resistant-gps-delayed-again-to-july-2025-at-earliest-pentagon-tester-says/.

133 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/.

134 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/.

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

136 Minnie Chan, "'Unforgettable humiliation' led to development of GPS equivalent," South China Morning Post, November 13, 2009, https://www.scmp.com/article/698161/unforgettable-humiliation-led-development-gps-equivalent.

137 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.

138 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/.

139 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/.

140 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/.

141 Chris Shieff, "Signal Jam: US GPS Interference Testing This Month," OpsGroup, March 14, 2022, https://ops.group/blog/signal-jam-us-gps-interference-testing-this-month/.

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

142 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/.

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 (e.g., command & control, relay of intelligence and operational data, control of UAVs) the employment of CCS in theater 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, is 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 or spoofing 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.[142] It is much more likely that an EW counterspace weapon would degrade military space capabilities rather than completely deny them.

1.4 — US 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 United States 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. The Missile Defense Agency (MDA) is planning to conduct research into the feasibility of DEW for defending against ballistic missiles and the Space Force has expressed an interest in a directed energy architecture in general (not necessarily space-based). 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 /
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.

The following paragraphs provide a general overview of different types of DEW capabilities as related to counterspace applications that apply to all the country-specific DEW sections in this report.

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 consumption of chemicals or electrical power. Space-based systems, on the other hand, could 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, several essential technological building blocks must be developed in order to field a high-power laser that will have an effective counterspace capability:

1. High fidelity space situational awareness,
2. High power laser device,
3. Precise beam tracking and control, and
4. 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:

1. Dazzling of a satellite's imaging sensor,
2. Damage to a satellite's imaging sensor, and
3. 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 sensor's 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 to completely clear the electric charge that was induced by the laser. Therefore, the effect may impact a plethora of images, following the laser incident. However, this effect is considered temporary since it will eventually clear on its own with no operator intervention. Laser dazzling could be used as a countermeasure 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.[143]

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 retroreflectors. 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.[144] 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 satellite's optics if it was pointed at the laser during a pulse.[145] Ultimately, the most difficult aspect of laser dazzling is not

143 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.

144 Ibid.

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

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

the power of the laser, but the 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 permanently damaged, 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.[146]

In the case of damage to optical sensors, the satellite will not otherwise be damaged. It can continue to be controlled and operated 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 very high-powered laser system.

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.

US Specific Directed Energy Weapons Program for Counterspace

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 is 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 US 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 (see Imagery Appendix, pg. 16-25). The project was initially funded by the Strategic Defense

146 Ibid.

Initiative Office (SDIO) beginning in 1985, with the goal of conducting research on ballistic missile defense.[147] MIRACL was fired against an orbiting satellite in October 1997, with then Secretary of Defense William Cohen putting out a statement that the test was "fully consistent" with US policy and did not violate international law.[148] 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 US satellites" and the Pentagon further stated that "there's absolutely no intention to use the laser for offensive purposes." [149]

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-2000s.[150] 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 US Army's White Sands Missile range.[151]

Another notable example was the Low-Power Atmospheric Compensation Experiment (LACE) satellite, launched in 1990, which was a Naval Research Laboratory project sponsored by the 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 were 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 (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 canceled in 2011. This project did not have a counterspace objective and did not directly develop capabilities to target satellites, although some technologies may have been 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 no publicly available evidence to suggest that the United States currently has space-based laser counterspace capabilities and there are likely significant technological obstacles to fielding such capabilities. 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.[152] The experiment was deemed successful because 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

147 White Sands Missile Range, "High Energy Laser Systems Test Facility," updated October 26, 2018, https://www.wsmr.army.mil/testcenter/testing/landf/Pages/HighEnergyLaserSystem-sTestFacility.aspx.

148 "Army to fire laser at satellite in space," *Tampa Bay Times*, Oct. 3, 1997, https://www.tampabay.com/archive/1997/10/03/army-to-fire-laser-at-satellite-in-space/.

149 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.

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

151 White Sands Missile Range, "High Energy Laser Systems Test Facility," updated October 26, 2018, https://www.wsmr.army.mil/testcenter/testing/landf/Pages/HighEnergyLaserSystem-sTestFacility.aspx.

152 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.

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 at short ranges for stopping, deterring, and turning back suspicious individuals with minimal risk of injury.[153] 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.

In October 2003, the US Air Force awarded an additional $32.2 million contract to Northrop Grumman to develop the Counter Surveillance and Reconnaissance System (CSRS, pronounced "scissors"), a mobile system that was intended to develop reversible means to temporarily dazzle space-based surveillance and reconnaissance satellites.[154] This was on top of an earlier award of $15 million. At the time the add-on contract was awarded, the goal was to get the work finished by October 2004; by July 2004, that had been pushed back to striving to reach initial operational capability by FY2009.[155] But the FY2005 Defense appropriations bill, finalized in August 2004, cut the entire funding for the program, with the Senate report noting that the Air Force had decided to stop the program.[156]

Current US DEW Developments and Capabilities

The US 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.[157] While none of these prototypes can be used for a counterspace role, they are furthering the development of component technologies that may apply 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 space-based missile defense initiatives that could also have counterspace applications. The SDIO transitioned into the Ballistic Missile Defense Organization (BMDO) in 1994, and 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 directed the DoD to study space-based defenses, which may include on-orbit demonstrations of concepts and technology.[158] Although the funding that may 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.[159] The MDA's budget request for 2020 included $34 million for neutral particle beam and laser technologies, with plans for testing a neutral particle beam weapon in orbit by 2023; however, the House version of the defense authorization act for that year asked for an in-depth study first and in September 2019, the Pentagon announced that it was "deferring work on neutral particle beams indefinitely."[160]

153 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.

154 Frank Tiboni, "Air Force seeks satellite blinder plans," *FCW*, October 24, 2003, https://fcw.com/workforce/2003/10/air-force-seeks-satellite-blinder-plans/224950/.

155 John A. Tirpak, "Securing the Space Arena," *Air Force Magazine*, July 1, 2004, https://www.airforcemag.com/artcle/0704space/.

156 Adolfo J. Fernandez, "Military Role in Space Control: A Primer," *Congressional Research Service Report RL32602*, September 23, 2004, https://sgp.fas.org/crs/natsec/RL32602.pdf.

157 *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.

158 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.

159 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/.

160 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/News/Transcripts/Transcript-View/Article/1784150/department-of-defense-press-briefing-on-the-presidents-fiscal-year-2020-defense/; Oriana Pawlyk, "Pentagon Halts Work on Directed-Energy Beam to Stop Enemy Missiles," Military.com, September 4, 2019, https://www.miitary.com/daily-news/2019/09/04/pentagon-halts-work-directed-energy-beam-stop-enemy-missiles.html.

It is not clear if the proposed studies into space-based defenses would 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 would address boost phase intercept,[161] that limitation is not specified in the 2022 Missile Defense Review, which does not mention lasers at all,[162] nor in the budget request information that has been made public.

The difference between boost phase and midcourse phase concepts is significant for ASAT capability. The tracking and pointing requirements 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. 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.

In June 2021, then Space Force Chief of Space Operations General John "Jay" Raymond was asked during a Congressional hearing whether the United States was working on a DEW portfolio "to be an effective capability for space dominance;" his response was, "Yes sir, we are.... We have to be able to protect these capabilities that we rely so heavily on." [163] A Space Force spokesperson explained later in a statement that Raymond's response "was confirming that our architecture developments in the face of these threats are appropriate."

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 the 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 a 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.

161 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/.

162 2022 Missile Defense Review, U.S. Department of Defense, October 27. 2022, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.

163 Nathan Strout, "The Space Force wants to use directed-energy systems for space superiority," C4ISRNet.com, June 16, 2021, https://www.c4isrnet.com/battlefield-tech/space/2021/06/16/the-space-force-wants-to-use-directed-energy-weapons-for-space-superiority/.

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

1.5 — US SPACE SITUATIONAL AWARENESS CAPABILITIES

Assessment /

The United States currently possesses the most advanced SSA capabilities in the world, particularly for military applications. US 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 SSA capabilities.

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 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 are their ability to cover large areas quickly and track objects above 5,000 km in 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 activities in space.

The United States, like Russia, developed its original SSA capabilities as part of the Cold War space and nuclear rivalry. The US 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 (see Imagery Appendix, pg. 16-32). 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 (see Imagery Appendix, pg. 16-31) 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, which was 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 (see Imagery Appendix, pg. 16-33).

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 (see Imagery Appendix, pg. 16-35), and the Reagan Test Site on Kwajalein Atoll in the South Pacific (see Imagery Appendix, pg. 16-37), along with optical telescopes. These include the Ground-Based Electro-Optical Deep Space Surveillance (GEODSS) system, which features triplets of 1-m optical telescopes located at Socorro, New Mexico, Diego Garcia atoll in the Indian Ocean, and the USAF Maui Optical and Supercomputing observatory in Hawaii (see Imagery Appendix, pg. 16-41).

In 2020, L3Harris won a 10-year, $1.2-billion contract for the Maintenance of Space Situational Awareness Integrated Capabilities (MOSSAIC). program to upgrade the capabilities of the GEODSS sensors and expand the number of telescopes and locations.[164] In October 2023, L3Harris announced it had won two contracts worth $134 million in support of its MOSSAIC work.[165]

Several efforts are underway to develop new capabilities for 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 (see Imagery Appendix, pg. 16-39) in March 2017.[166] The Space Surveillance Telescope (SST), a 3.5-meter telescope originally developed by DARPA, was also moved to Naval Communication Station Holt (see Imagery Appendix, pg. 16-40) to be jointly operated by the USAF's Space Delta 2 unit and the Royal Australian Air Force.[167] It imaged its first objects in March 2020 and was declared operational in September 2022.[168]

The USAF also has the Space Fence program to develop new S-Band phased arrays to improve tracking of small objects as a replacement for the Navy Space Surveillance System (NAVSPASUR) that was shuttered in 2013. The first S-Band Space Fence was constructed on Kwajalein Atoll (see Imagery Appendix, pg. 16-34), which is anticipated to be able to track small space objects down to a few centimeters.[169] The USAF envisioned a second Space Fence site in the future, but no funding has yet been made.

Another new radar program, the Deep Space Advanced Radar Capability (DARC), was awarded to Northrop Grumman in February 2022 to build the first of an anticipated three new radars capable of tracking objects in deep space.[170] In May 2023, the Space Force announced it would start construction on the first of three sites for the DARC program with the goal of completing that first site's construction by the end of 2025; the three sites are expected to be in the United States, Australia, and the United Kingdom.[171] The second and

164 Sandra Erwin, "L3Harris Wins $1.2 billion Contract to Maintain, Upgrade Space Surveillance Systems," *SpaceNews*, February 29, 2020, https://spacenews.com/l3harris-wins-1-2-billion-contract-to-maintain-upgrade-space-surveillance-sensors.

165 "L3HARRIS To Advance Department Of Defense's Space Domain Awareness Mission," L3Harris, October 19, 2023, https://www.l3harris.com/newsroom/press-release/2023/10/l3harris-advance-department-defenses-space-domain-awareness-mission.

166 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/.

167 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/; Sandra Erwin, "Space surveillance telescope developed by the U.S. begins operations in Australia," *SpaceNews*, September 30, 2022, https://spacenews.com/space-surveillance-telescope-developed-by-the-u-s-begins-operations-in-australia/.

168 "Joint US-Australian Space Surveillance Telescope To Be Improved," Australian Defence Magazine, July 16, 2020, https://www.australiandefence.com.au/defence/cyber-space/joint-us-australian-space-surveillance-telescope-to-be-improved; Erwin, September 30, 2022, ibid.

169 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/.

170 Sandra Erwin, "Northrop Grumman win $341 million Space Force contract to develop a deep-space tracking radar," *SpaceNews*, February 23, 2022, https://spacenews.com/northrop-grumman-wins-341-million-space-force-contract-to-develop-a-deep-space-tracking-radar/.

171 Apurva Minchekar, "Space Force to start DARC Site 1 construction," Inside Defense, May 10, 2023, https://insidedefense.com/insider/space-force-start-darc-site-1-construction.

third sites are planned to be completed in 2028 and 2029, for which the Space Force announced in August 2023 that it would be releasing a sole-source request for proposal to Northrop Grumman.[172] In October 2023, the SSC announced "Project Apollo," an effort to spur three-month innovation cycles in solving major SSA issues; the first one to be examined was misidentification of objects that could actually be threat intelligence payloads or weapons.[173]

In addition to ground-based sensors, the US SSN also includes multiple space-based optical sensors. The Space-Based Space Surveillance (SBSS) satellite is in LEO and has a large, gimbaled telescope that can track space objects in higher orbits.[174] The Canadian Sapphire satellite is a smaller satellite in a similar orbit that also contributes to the SSN.[175] The USSF also operates GSSAP satellites in GEO, which can provide up-close imaging, characterization, and intelligence (see US Co-Orbital ASAT; Section 1.2). ORS-5 SensorSat (2017-050A, 42921) was launched in 2017 and became operational in 2019.[176] It keeps an eye on GEO from a LEO orbit of 591 km by 575 km.[177] TDO-2 (2020-022A, 45464) 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.[178]

A classified space-based SSA system called "SILENT BARKER" is being jointly developed by the USSF and the NRO; it was initially to have been launched in 2022, but a problem was discovered during launch preparation, so the satellite was returned to its manufacturer and the launch rescheduled for August 2023.[179] The mission actually ended up being launched in September 2023, with three satellites designated USA 346 (2023-140A, 57836), USA 347 (2023-140B, 57837), and USA 348 (2023-140C, 57838) being placed into orbit above GEO at 12 degree inclination.[180] NRO Deputy Director Maj. Gen. Christopher Povak explained the difference between SILENT BARKER and GSSAP thus: "SILENT BARKER is looking at the entirety of that geosynchronous belt consistently. And GSSAP is responsible for doing characterization to detect anomalies or provide intricate characterization of satellites in geosynchronous orbit;" it might be used for targeting from space, but it is hard to say at this point.[181]

An unnamed space-based SSA program with three novel sensor payloads developed by the Space Rapid Capabilities Office (SpRCO) was launched in January 2023 by the Space Force; according to SpRCO, the payloads "fly around GEO and collect data about potential threats on-orbit." [182] The payloads are likely attached to the Long Duration EELV Secondary Payload Adapter (LDPE) 3A (USA 342, 2023-008A, 55263), which also hosts two other technology demonstration payloads for the USSF.[183]

172 Sandra Erwin, "Northrop Grumman to get sole-source contract for Space Force radar sites," ***SpaceNews***, August 17, 2023, https://spacenews.com/northrop-grumman-to-get-sole-source-contract-for-space-force-radar-sites/.

173 Frank Wolf, "U.S. Space Force "Project Apollo" to Help Unveil Adversary Cloaking in Space," Defense Daily, October 11, 2023, https://www.defensedaily.com/u-s-space-force-project-apollo-to-help-unveil-adversary-cloaking-in-space/space/.

174 "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/.

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

176 "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/.

177 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.

178 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/.

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

180 Courtney Albon, "Space Force, NRO launch 'Silent Barker' space observation satellites, C4ISRNet, September 10, 2023, https://www.c4isrnet.com/battlefield-tech/space/2023/09/10/space-force-nro-launch-silent-barker-space-observation-satellites/.

181 Greg Hadley, "NRO, Space Force Partner to Craft New Moving Targeting Strategy," Air & Space Forces Magazine, October 10, 2023, https://www.airandspaceforces.com/nro-space-force-partnership-targeting-strategy/.

182 Theresa Hitchens, "Space Force's new, classified 'threat warning' sensors now delivering intel on 'foreign capabilities'," Breaking Defense, December 14, 2023, https://breakingdefense.com/2023/12/space-forces-new-classified-threat-warning-sensors-now-delivering-intel-on-foreign-capabilities/.

183 Gunter Krebs, "LDPE 1, 2, 3A (ROOSTER 1, 2, 3A)," Gunter's Space Page, April 23, 2023, https://space.skyrocket.de/doc_sdat/ldpe-1.htm.

In April 2019, the head of the Space Development Agency announced they were exploring architectures for extending SSA out to cislunar space.[184] AFRL's Space Vehicles Directorate is also considering what it calls "xGEO" orbits, those beyond GEO out to cislunar space, with the goal of extending SDA from GEO out past the Moon.[185] 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.[186] In December 2021, AFRL announced its support of a research project called "Space Object Understanding and Reconnaissance of Complex Events (SOURCE)," which is intended to help improve SSA modeling of the xGEO domain.[187]

The data from the SSN sensors is collated and processed by the 18th Space Defense Squadron (18 SDS), located at Vandenberg Space Force Base in California.[188] 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.[189] An alternate command center is located in Dahlgren, Virginia, at what used to be the control facility for the NAVSPASUR. In April 2022, the unit at Dhalgren was renamed the 19th Space Defense Squadron (19 SDS) with a new focus on xGEO SDA.[190] Both report to Space Delta 2, garrisoned at Peterson SFB, Colorado.[191]

A significant portion of the satellite catalog maintained by the 18th SDS and SSA analysis products such as conjunction assessments and re-entry predictions are made publicly available on the Space Track website.[192] Efforts to improve the software and computer systems used by the 18th SPCS have run into long-standing problems and delays.[193] In January 2022, the USSF shut down the Joint Space Operations Center Mission System (JMS) program, which was intended to improve SSA but was instead beleaguered by delays and cost overruns.[194] Currently, the USSF is pursuing multiple new programs to try and upgrade or replace the legacy computer systems still being used for the operational SSA mission.[195]

184 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/.

185 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/.

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

187 Theresa Hitchens, "AFRL jumpstarts early research on cislunar monitoring, satellite servicing," *Breaking Defense*, December 17, 2021, https://breakingdefense.com/2021/12/afrl-jumpstarts-early-research-on-cislunar-monitoring-satellite-servicing/.

188 "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/.

189 "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/.

190 Theresa Hitchens, "The USSF stood up the 19th Space Defense Squadron in April 2022 so it can track objects in xGEO space," BreakingDefense, April 21, 2022, https://breakingdefense.com/2022/04/to-infinity-and-beyond-new-space-force-unit-to-monitor-xgeo-beyond-earths-orbit/.

191 Stephen Brady, "Space Delta 2 monitors deep space," Peterson Space Force Base Press Release, accessed February 20, 2022, https://www.peterson.spaceforce.mil/News/Article/2564700/space-delta-2-monitors-deep-space/.

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

193 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.

194 Sandra Erwin, "Space Force's troubled space-tracking system is officially shut down," *Space News*, January 27, 2022, https://spacenews.com/space-forces-troubled-space-tracking-system-is-officially-shut-down/.

195 Theresa Hitchens, "Seeing in the dark: Space Force works, slowly, to improving monitoring of the heavens," *Breaking Defense*, April 5, 2022, https://breakingdefense.com/2022/04/seeing-in-the-dark-space-force-works-slowly-to-improve-monitoring-of-the-heavens/.

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.[196] A main function of the NSDC is to leverage military and commercial SSA capabilities to detect and characterize attacks on US national security satellites.[197]

As of February 2024, the United States military has signed 170 SSA data sharing agreements with 34 countries, 142 companies, and 7 universities, as well as as well as foreign and intergovernmental agencies.[198] The primary purpose of these agreements is to enable the US 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 a two-way exchange of SSA data between the parties. 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 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.[199] An updated version was issued by the Trump administration in 2019.[200]

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 US SSN possesses 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.

1.6 — US 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 US 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. Current US military doctrine includes space domain awareness and offensive and defensive space operations as among the primary mission areas for joint actionf and "suppression of enemy space capabilities"as the goal for its offensive space operations.

The United States has reorganized its military space activities as part of a renewed focus on space as a warfighting domain. Since 2014, US 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

196 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/.

197 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/.

198 Emily Peacock, "Congressional Fellowship Group Visits Space Delta 2's 18th Space Defense Squadron," *Defense Visual Information Distribution System*, February 5, 2024, https://www.dvidshub.net/news/463224/congressional-fellowship-group-visits-space-delta-2s-18th-space-defense-squadron; "USSPACECOM, CONIDA, and the Peruvian Air Force sign SSA," US Space Command Press Release Release No. 2023-04-01, April 18, 2023, https://www.spacecom.mil/Newsroom/News/Article-Display/Article/3367184/usspacecom-conida-and-the-peruvian-air-force-sign-ssa/.

199 "National Space Weather Action Plan," N*ational Science and Technology Council*, October 2015, https://www.sworm.gov/publications/2015/swap_final__20151028.pdf.

200 "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.

in the reestablishment of US Space Command (USSPACECOM) and the creation of the US Space Force (USSF), which assumed the responsibilities of US Strategic Command for space warfighting and Air Force Space Command (AFSPC) for operating, training, and equipping of space forces, respectively. To date, the missions of these new organizations are largely a continuation of previous military space missions, although some have advocated for expanding their focus to include cislunar activities and more offensive weapons. It is likely that the United States has also begun developing new offensive counterspace capabilities, although the United States has publicly stated it will not test destructive DA-ASAT weapons. The United States also continues to hold annual space wargames and exercises that increasingly involve close allies and commercial partners.

Specifics /

US 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 US 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 or war.[201] The goal was not to deter the Soviets from attacking US 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 US satellites to those in LEO. The memos specifically highlighted the use of Soviet space systems for targeting long-range anti-ship missiles against US 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.[202] The ASAT capability eventually became the ASM-135 missile launched from an F-15 fighter aircraft.

More recent US 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."[203]

In December 2021, the Biden administration unveiled its Space Priorities Framework, which states, "The United States will defend its national security interests from the growing scope and scale of space and counterspace threats.... To deter aggression against US, allied, and partner interests in a manner that contributes to strategic stability, the United States will accelerate its transition to a more resilient national security space posture and strengthen

201 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.

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

203 "National Space Policy of the United States of America," T*he White House*, December 9, 2020, p. 4, https://web.archive.org/web/20201209213138/https://www.whitehouse.gov/wp-content/uploads/2020/12/National-Space-Policy.pdf.

its ability to detect and attribute hostile acts in space. The United States also will take steps to protect its military forces from space-enabled threats."[204]

US Military Doctrine on Counterspace

The link between these policy statements and offensive counterspace capabilities can be found in the official US military doctrines on space operations. Two different historical doctrines existed on space operations: an Air Force doctrine developed by AFSPC;[205] and a joint doctrine developed by United States Strategic Command (Joint Publication 3-14 (JP 3-14): Joint Space Operations).[206] The most recent publicly available versions of these doctrines are August 2018 and October 2020, respectively. However, JP 3-14 was reported to have been updated in August 2023, and while it is officially unclassified, DoD officials have determined they wish to keep it within the Department as a "limited distribution publication."[207] The August 2023 update reportedly describes SPACECOM's area of responsibility as "astrographic", a term it created to describe 100 km above mean sea level to "exgeosynchronous" orbit, which it deems to include lunar and cislunar orbits, as well as the Lagrange points.[208] It includes space domain awareness and offensive and defensive space operations as among the primary mission areas for joint action. The doctrinal document describes how either direct or enabling capabilities support each mission area, and distinguishes the two as following: "The key discriminator between direct and enabling capabilities is whether it can impose a cost or not. If it does, it is a direct capability."[209] Finally, it gets rid of the terms "space control" and "counter-space," and sets out the goal of "suppression of enemy space capabilities" for its offensive space operations, as "space superiority" was reportedly deemed to be too much of a difficult end-state to describe or reach.[210]

In July 2023, the USSF released "Space Doctrine Publication 3-0, Operations" (SDP 3.0), to describe how the USSF Guardians will support USSPACECOM and the joint forces.[211] In the section detailed "Combat Power Projection," it talks about offensive and defensive military force, which it calls "fires and protection," and goes on to say that, "Offensive space operations attack the adversary in, from, or to space. These operations seek to impose cost on the adversary, compel a change in behavior, secure a position of advantage, or deny the adversary's military forces freedom of action. Defensive space operations seek to repel or defeat adversary attacks in, from, or to the space domain. These operations aim to maintain status quo, regain the initiative, deny the adversary a position of advantage, or protect freedom of action of friendly forces."[212] And in emphasizing the importance of joint all-domain operations, it notes that "the most effective operation to deny, disrupt, damage, or destroy an adversary's space capability, and preserve freedom of action in space, may originate from a domain other than space."[213] The new terms shift space doctrine to be more in line with how the US military describes joint operations in the land, air, and sea domains.

The USSF released its first space doctrine in June 2020 with its Space Capstone Publication which articulated how it views spacepower. Included in its guiding principles are that "[t]The U.S. must adapt its national security space organizations, doctrine, and capabilities to deter and defeat aggression and protect national interests in space," that spacepower is inherently global and multidomain, and that military space forces employ spacepower "in, from, and through the space domain" which necessitates "close collaboration and cooperation with the U.S. Government, Allies, and partners."[214]

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).[215] According

204 "United States Space Priorities Framework," *The White House*, December 2021, p. 6, https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Space-Priorities-Framework-_-December-1-2021.pdf.

205 "Counterspace Operations," *Annex 3-14 Counterspace Operations*, August 27, 2018, https://www.doctrine.af.mil/Doctrine-Publications/AFDP-3-14-Counterspace-Ops/.

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

207 Theresa Hitchens, "EXCLUSIVE: New Joint Force space doctrine clarifies Space Command's 'offensive', 'defensive' ops," Breaking Defense, October 27, 2023, https://breakingdefense.com/2023/10/exclusive-new-joint-force-space-doctrine-clarifies-space-commands-offensive-defensive-ops/.

208 Hitchens, "EXCLUSIVE: New Joint Force space doctrine," ibid.

209 Hitchens, "EXCLUSIVE: New Joint Force space doctrine," ibid.

210 Hitchens, "EXCLUSIVE: New Joint Force space doctrine," ibid.

211 Space Doctrine Publication (SDP) 3-0, Operations Space Training and Readiness Command (STARCOM) OPR: STARCOM Delta 10 19 July 2023, https://www.starcom.spaceforce.mil/Portals/2/SDP%203-0%20Operations%20(19%20July%202023).pdf?ver=nHRhKpy49X-VtcSVRaQRNNg%3d%3d.

212 Ibid, p. 33.

213 Ibid, pp. 25-26.

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

215 Theresa Hitchens, "Exclusive: NRO, SPACECOM Craft CONOPS for War in Space," BreakingDefense, May 4, 2020, https://breakingdefense.com/2020/05/exclusive-nro-spacecom-craft-conops-for-war-in-space/.

to the NRO's deputy director, this is intended to "strengthen and synchronize our defensive operations" and to clarify who defends what.[216] For example, they worked together to develop a concept of operations for the SILENT BARKER SSA satellite network so that each organization could get the operational data that they wanted, and they have indicated that they will strive to do the same for developing a moving target indication (MTI) from space.[217]

The latest version of the Unified Command Plan (UCP 2022), which outlines the relationships between the combatant commands, was signed by President Biden in April 2023.[218] This document elucidates USSPACECOM's roles and responsibilities compared to the other combat commands.[219] The most recent version transferred missile defense responsibilities from USSTRATCOM to USSPACECOM: specifically, per US Army Gen. James Dickinson, USSPACECOM commander, "the three mission areas of missile warning, missile defense and space domain awareness" are now "under one command as the Global Sensor Manager."[220] While USSTRATCOM's Joint Functional Component Command for Integrated Missile Defense (JFCC IMD) will also transfer to USSPACECOM; a statement released by USSPACECOM noted that "USSTRATCOM along with U.S. Northern Command will retain and continue to perform the Integrated Threat Warning and Attack Assessment missions."[221]

Recent Policy Shifts

Since 2014, US 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),[222] which concluded there was a need to identify threats in space, be able to withstand aggressive counterspace programs, and counter adversary space capabilities.[223] 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.[224] There was also increased focus on preparing to "fight a war in space," even though senior US military leaders expressed no desire to start one.[225] In November 2021, General David Thompson, vice chief of space operations for the Space Force, encapsulated much of the besieged language US government officials have been using to describe the current state of space when he told a reporter that US satellites were being targeted by reversible attacks "every single day."[226] A shift in tone was also seen in academic writings from US military journals calling for renewed focus on fighting wars in space and offensive space control.[227] The US Congress also weighed in, calling in 2014 for a study on how to deter and defeat adversary attacks on US space systems, and specifically the role of offensive space operations.[228] This concern was echoed in the 2023 National Defense Authorization Act, released in December 2022, which acknowledged "the need to shift to a more resilient and defendable national security space architecture" and required DoD to create a "strategy and requirements for the protection of DoD satellites."[229]

216 Hitchens, May 4, 2020, ibid.

217 Greg Hadley, "NRO, Space Force Partner to Craft New Moving Targeting Strategy," Air & Space Forces Magazine, October 10, 2023, https://www.airandspaceforces.com/nro-space-force-partnership-targeting-strategy/.

218 2022 Unified Command Plan, A Presidential Document by the Executive Office of the President on 04/28/2023, https://www.federalregister.gov/documents/2023/04/28/2023-09182/2022-unified-command-plan.

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

220 "USSPACECOM Assumes Missile Defense Mission," USSPACECOM Press Release No. 2023-05-01, May 30, 2023, https://www.spacecom.mil/Newsroom/News/Article-Display/Article/3411944/usspacecom-assumes-missile-defense-mission/.

221 "USSPACECOM Assumes Missile Defense Mission," ibid.

222 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.

223 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.

224 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/.

225 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.

226 Josh Rogin, "Opinion: A shadow war in space is heating up fast," *Washington Post*, November 30, 2021, https://www.washingtonpost.com/opinions/2021/11/30/space-race-china-david-thompson/.

227 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; 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.

228 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.

229 Sandra Erwin, "NDAA compromise bill wants more focus on satellite protection, responsive launch," Space News, December 7, 2022, https://spacenews.com/ndaa-compromise-bill-wants-more-focus-on-satellite-protection-responsive-launch/.

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.[230] The aggressive rhetoric from the Trump administration increased in the latter half of 2018 and throughout 2019. In various speeches and rallies promoting the USSF, then President Trump called for the United States to "dominate" space. In his remarks during the signing ceremony for establishing the USSF, then 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.[231] Yet official US policy statements on space security issues issued by the Trump administration, or at least the public ones, continue to reflect a more moderate tone and did not explicitly outline the development of new offensive space weapons.[232]

In December 2021, Deputy Secretary of Defense Kathleen Hicks stated, "We would like to see all nations agree to refrain from anti-satellite weapons testing that creates debris,"[233] leading to some speculation that the United States might be soon supporting an ASAT test moratorium. The United States did indeed formally announce in April 2022 that it was making the commitment not to conduct destructive anti-satellite missile tests.[234] As of October 2023, 37 countries have made that commitment.[235] The US State Department's "Strategic Framework for Space Diplomacy," released in May 2023, discusses goals for national security in order to "Promote US and allied security through bilateral and multilateral efforts that enhance capabilities and reduce risks of unintended conflict or escalation."[236]

The Department of Defense is also increasing its focus on resiliency and norms of behavior as a way in which to also ensure its continued access to and use of space. In July 2021, Secretary of Defense Lloyd Austin released the first "Tenets of Responsible Behavior in Space," a set of norms that USSPACECOM would use to guide their military space operations.[237] In August 2022, an update to DoD Directive 3100.10, "Space Policy," was released that directed compliance with the tenets.[238] Directive 3100.10 also directed the DOD to develop and field capabilities that counter hostile uses of space; develop capabilities, resilient architectures, and options for capability reconstitution to "reduce vulnerabilities and deny benefits from attacking US space systems; and promote long-term sustainability of the space environment; cooperate with like-minded international partners to establish, demonstrate, and uphold norms of safe and responsible behavior; and cooperate with other US Government departments and agencies to act as a good steward of the domain."[239]

In November 2022, it was reported that the United States had finished its most recent Strategic Space Review, conducted jointly by the Director of National Intelligence and the Office of the Secretary of Defense, but that an unclassified version would not be released.[240] DoD officials were able to broadly discuss what it included: listed as priorities were for the DoD to, in the words of Assistant Secretary of Defense for Space Policy John Plumb, "build a resilient national security space architecture" and "lead in the responsible and peaceful use of space," as part of its guidance "to protect and defend our national security interests" against counterspace attacks.[241]

In February 2023, USSPACECOM released an updated version of the tenets that added eight specific proposed behaviors for the Department of Defense's operations in the space area of responsibility.[242]

In March 2023, General Chance Saltzman, Chief of Space Operations unveiled the broad strokes of a new "theory of success" for the USSF through a

230 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.

231 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.

232 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.

233 Michael Sheetz, "Pentagon calls for stop to anti-satellite weapons testing after Russian demo debris threatened ISS," *CNBC*, December 1, 2021, Pentagon calls for stop to anti-satellite weapons testing (cnbc.com).

234 "Fact Sheet: Vice President Harris Advances National Security Norms in Space,," White House, April 18, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/18/fact-sheet-vice-president-harris-advances-national-security-norms-in-space/.

235 "Multilateral Space Security Initiatives," Secure World Foundation, last updated November 13, 2023, https://swfound.org/multilateral-space-security-initiatives/.

236 A Strategic Framework for Space Diplomacy, U.S. Department of State, May 2, 2023, p. 25, https://www.state.gov/wp-content/uploads/2023/05/Space-Framework-Clean-2-May-2023-Final-Updated-Accessible-5.25.2023.pdf.

237 Lloyd Austin, "Tenets of REsponsible Behavior in Space," U.S. Department of Defense, July 7, 2021, https://media.defense.gov/2021/Jul/23/2002809598/-1/-1/0/TENETS-OF-RESPONSIBLE-BEHAVIOR-IN-SPACE.PDF.

238 DoD Directive 3100.10: Space Policy, August 30, 2022, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/310010p.PDF.

239 DoD Directive 3100.10: Space Policy, ibid.

240 Theresa Hitchens, "EXCLUSIVE: US Strategic Space Review signed out, but no unclassified version is coming," *Breaking Defense*, November 1, 2022, https://breakingdefense.com/2022/11/exclusive-us-strategic-space-review-signed-out-but-no-unclassified-version-is-coming/.

241 Sandra Erwin, "U.S. national security space strategy emphasizes resilient systems, responsible behavior," *SpaceNews*, December 14, 2022, https://spacenews.com/u-s-national-security-space-strategy-emphasizes-resilient-systems-responsible-behavior/.

242 Lloyd Austin, "Tenet Derived Responsible Behaviors in Space," U.S. Department of Defense, February 9, 2023, https://www.spacecom.mil/Newsroom/Publications/Pub-Display/Article/3318615/tenet-derived-responsible-behaviors-in-space/.

"Commander's Note" issued to the service.[243] General Saltzman stated that the formative purpose of the USSF was to "contest, and when directed, control the space domain on behalf of the joint force." In doing so, the USSF needed to focus on three core tenets: space domain awareness, using resilience to deter attack, and 'responsible' counterspace activities that avoided destruction of satellites that would create orbital debris. He followed this up with "Competitive Endurance: A Proposed Theory of Success for the Space Force," in January 2024, which defines space superiority as the ability to "employ space capabilities in support of military objectives while also preventing adversaries from using their own."[244] It echoes his earlier document on the three core tenets for this theory of success: avoiding operational surprise, denying first-mover advantage, and undertaking responsible counterspace campaigning.[245] The latter refers to how the USSF plans to achieve its space offensive and defensive space operations needs while avoiding destruction of satellites that would create large amounts of orbital debris.

DoD released its Space Policy Review and Strategy of Protection of Satellites in September 2023, done in response to Congressional legislation requiring it.[246] The review gave an assessment of threats to the space environment, focusing on China and Russia and clarified how DoD plans to defend against threats: "Assure critical space-based missions by accelerating the transition to more resilient architectures and by protecting and defending critical systems against counterspace threats; Strengthen the ability to detect and attribute hostile acts in, from, and to space; and Protect the Joint Force from adversary hostile uses of space."[247] It discussed the need to "deter aggression and, if deterrence fails, to prevail in conflict," and stated that DoD would "balance the development, testing, and employment of these capabilities with our need to maintain a stable and sustainable space environment."[248] It also had a section on normative behaviors in space, noting, "In collaboration with the Department of State, the Department of Defense is committed to promoting standards and norms that ensure the domain remains secure, stable, and accessible."[249]

US Space and Counterspace Organization

Since the early 2000s, there had been an on-going debate about the organization of US military space activities. The recruit, train, and equip functions normally done by a service were assigned to the Department of the Air Force, and the operational warfighting functions were assigned to US Strategic Command (USSTRATCOM). In the 2010s, the debate was revitalized by the increased concern expressed above over adversary counterspace capabilities, and also a desire to increase coordination with allies and commercial partners. 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.[250] 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.[251] New Zealand was added in 2015; France and Germany joined in 2019; and Italy, Japan, and Norway came on-board in December 2023.[252] In addition to maintaining their own national centers, US Strategic Command's JSpOC was renamed the CSpOC and included CSpO exchange officers and a Commercial Integration Cell (CIC).[253]

243 Theresa Hitchens, "Space Force chief outlines 3-part 'competitive endurance' theory aimed at 'space superiority'," Breaking Defense, March 7, 2023, https://breakingdefense.com/2023/03/space-force-chief-outlines-3-part-competitive-endurance-theory-aimed-at-space-superiority/.

244 Todd Harrison, "Where the Space Force's new 'theory of success' succeeds," Defense One, January 22, 2024, https://www.defenseone.com/ideas/2024/01/where-space-forces-new-theory-success-succeeds/393526/.

245 Todd Harrison, "Where the Space Force's new 'theory of success' succeeds," ibid.

246 Space Policy Review and Strategy on Protection of Satellites, Submitted in compliance with the reporting requirements contained in Section 1611 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2022 & Section 1602 of the NDAA for FY 2023, U.S. Department of Defense, September 2023, https://media.defense.gov/2023/Sep/14/2003301146/-1/-1/0/COMPREHENSIVE-REPORT-FOR-RELEASE.PDF.

247 Space Policy Review and Strategy on Protection of Satellites, p. 7.

248 Ibid.

249 Space Policy Review and Strategy on Protection of Satellites, p. 13.

250 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.

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

252 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/; David Vergun, "More Nations Meet to Address Space Security," DoD News, December 7, 2023, https://www.defense.gov/News/News-Stories/Article/Article/3610656/more-nations-meet-to-address-space-security/.

253 "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.

The organizational debate came to a head in the mid-2010s when the US Congress 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.[254] Then 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.[255] But Space Policy Directive (SPD)-4, released by the Trump administration in February 2019, settled on a more moderate approach that would create the Space Force as a new military service within the Department of the Air Force.[256] Separately, there were also calls to resurrect US Space Command (USSPACECOM) as the combatant command to take over space warfighting duties from USSTRATCOM.[257]

USSPACECOM was officially re-established as the 11th combatant command on August 29, 2019, in a ceremony at the White House Rose Garden.[258] General Raymond was named as Commander of USSPACECOM, which was established as a geographic combatant command with authority for all US military operations above 100 km altitude.[259] The mission of USSPACECOM is to deter aggression and conflict, defend US and allied interests, deliver space combat power, and develop ready and lethal joint warfighters.[260] Initially, USSPACECOM was intended to consist of two subordinate commands, each of which was composed of several already existing commands and operations centers. Combined Force Space Component Command (CFSCC) plans, tasks, directs, monitors, and assesses the execution of combined and joint space operations for theater effects. The Joint Task Force Space Defense (JTF-SD), in unified action with mission partners, deters aggression, defends capabilities, and defeats adversaries throughout the continuum of conflict. Schriever Space Force Base in Colorado.[261] The two (JTF-SD and CFSCC) were combined in December 2024 into the US Space Forces-Space Command, which is intended to organize, train, and equip forces for the USSF and oversee all space forces for USSPACECOM.[262] In November 2021, General James Dickinson, commander of USSPACECOM, signed off on the creation of a new operational component command, the Combined Joint Task Force-Space Operations (CJTF-SO), which will eventually combine JTF-SD and CFSCC to streamline reporting chains under USSPACECOM and USSF.[262] In May 2020, General Raymond signed the first operations order as Commander of USSPACECOM for Operation Olympic Defender (OOD), USSPACECOM's plan to protect US and allied satellites during a conflict.[263] OOD was created by USSTRATCOM in 2013 and opened for ally participation in 2018.[264] The United Kingdom became the first ally to join OOD in July 2019.[265]

The USSF was formally created on December 20, 2019, with then President Trump's signing of the Fiscal Year 2020 National Defense Authorization Act.[266] The signing followed 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 then President Trump wanted in June 2018.[267] 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 consisted only of members of the USAF and was stood up over 18 months, beginning by re-designating AFSPC as the USSF. The USSF has about 8,100 personnel as of February 2023,[268] but is planned to eventually grow to 16,000.

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

255 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.

256 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.

257 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.

258 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/.

259 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/.

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

261 Ibid.

262 Sandra Erwin, "Space Force reorganizes command structure to streamline operations," *SpaceNews*, December 13, 2023, https://spacenews.com/space-force-reorganizes-command-structure-to-streamline-operations/.

263 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/.

264 Hitchens, May 21, 2020, ibid.

265 "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/.

266 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.

267 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.

268 Rachel Cohen, "New in 2023: Saltzman leads Space Force into its 4th year," *Air Force Times*, January 3, 2023, https://www.airforcetimes.com/news/your-air-force/2023/01/03/new-in-2023-saltzman-leads-space-force-into-its-4th-year/.

The USSF is organized into multiple commands: training is handled by the Space Training and Readiness Command (STARCOM); operations by Space Operations Command (SpOC); and acquisitions by Space Systems Command (SSC).[269] Within each command are a number of Space Deltas, many of which are rebranded space operations squadrons that formerly existed under AFSC. The Space Warfighting Analysis Center (SWAC) is a direct reporting unit intended to develop "force design" for USSF mission areas, like ISR or missile warning and tracking, and is headquartered in Washington, DC.[270]

STARCOM was activated in August 2021 and is charged with training the Guardians (what members of the USSF are called), building out space doctrine and tactics, and establishing testing and evaluation of the USSF.[271] As part of this training, STARCOM is looking at what level of baseline capability is needed for the USSF's National Space Test and Training Complex (NSTTC), which would help provide realistic training for Guardians.[272]

SSC is based on Air Force Space Command's Space and Missile Systems Center and is headquartered at Los Angeles Air Force Base in California. SSC announced a reorganization in March 2022 that is intended to help acquisitions become better integrated and to pivot significantly to a resilient architecture."[273] The USSF created the Space Force Acquisition Council as part of its efforts to carry out the responsibilities of being designated the lead integrator for joint space requirements; representatives from the SSC, MDA, and NRO, among others, discuss their programs with the goal of making their work complementary.[274]

USSF is also actively developing dedicated space intelligence capabilities. In October 2021 the Space Force Intelligence Activity (SFIA) was created as an interim step until the National Space Intelligence Center is eventually stood up by the USSF.[275] Space Force Delta 18 was created in June 2022 to be able to provide intelligence on threats and foreign space capabilities to US policy-makers; it will run the National Space Intelligence Center at Wright-Patterson Air Force Base in Ohio.[276] Space Delta 7 activated its 75th Intelligence, Surveillance and Reconnaissance Squadron (ISRS) in August 2023 as the first targeting unit supporting the USSF; it has three missions: "target analysis, target development and target engagement."[277]

Both the USSF and USSPACECOM have also taken specific organizational steps to address the cyber security of space capabilities. In April 2021, USSPACECOM announced it was standing up a Joint Cyber Center to focus on cybersecurity of satellites and space-based communications and to help it integrate with other DoD cyber organizations.[278] In May 2021, the Space Systems Command of the USSF stated it was developing a digital twinning technology to improve the cyber security of future military space architectures.[279] The USSF's Space Delta 6 (the "Cyber" Delta) was planning to expand the number of squadrons it had in summer 2022 so it could provide nearly all the other Space Deltas with cyber squadrons to protect their mission systems.[280] In general, cybersecurity is a serious concern for the USSF: Space Operations Command (SpOC) head Lieutenant General Stephen Whiting called cybersecurity "the soft underbelly of these global space networks."[281]

269 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/.

270 Theresa Hitchens, "Exclusive: Space acquisition shop set for another re-org, following Congress-backed SWAC model," *BreakingDefense*, December 20, 2021, https://breakingdefense.com/2021/12/exclusive-space-acquisition-shop-set-for-another-re-org-following-congress-backed-swac-model/.

271 "Space Force activates Space Training and Readiness Command," *AFNS*, August 24, 2021, https://www.spacewar.com/reports/Space_Force_activates_Space_Training_and_Readiness_Command_999.html.

272 Courtney Albon, "Space Force envisions digital future for testing and training," *C4ISRNet.com*, June 15, 2022, https://www.c4isrnet.com/battlefield-tech/space/2022/06/15/space-force-envisions-digital-future-for-testing-and-training/.

273 Sandra Erwin, "Raymond: Space Force in 2022 to focus on the design of a resilient architecture," *SpaceNews*, January 18, 2022, https://spacenews.com/raymond-space-force-in-2022-to-focus-on-the-design-of-a-resilient-architecture/.

274 Nathan Strout, "Space enterprise more unified than ever, says Space Force chief," Defense News, September 21, 2021, https://www.defensenews.com/battlefield-tech/space/2021/09/21/space-enterprise-more-unified-than-ever-says-space-force-chief/.

275 Sandra Erwin, "Space Force intelligence organization established at Wright Patterson Air Force Base," *SpaceNews*, October 4, 2021, https://spacenews.com/space-force-establishes-intelligence-analysis-organization-at-wright-patterson-air-force-base/.

276 Sandra Erwin, "Space Force establishes intelligence unit to put sharper focus on orbital threats," *SpaceNews*, June 24, 2022, https://spacenews.com/space-force-establishes-intelligence-unit-to-put-sharper-focus-on-orbital-threats/.

277 Cody Friend, "Space Force's first targeting squadron brought to life," Defense Visual Information Delivery Service, August 11, 2023, https://www.dvidshub.net/news/451367/space-forces-first-targeting-squadron-brought-life.

278 Jackson Barnett, "Space Command to launch Joint Cyber Center," *FedScoop*, April 20, 2021, https://www.fedscoop.com/space-command-joint-cyber-center/.

279 Shaun Waterman, "Space Force Looks to Boost Cyber Defenses of Satellites with Acquisition Reorganization," *Air Force Magazine*, May 10, 2021, https://www.airforcemag.com/space-force-looks-to-boost-cyber-defenses-of-satellites-with-acquisition-reorganization/.

280 Theresa Hitchens, "Space Force adding new cyber squads, improving satellite control," *Breaking Defense*, May 27, 2022, https://breakingdefense.com/2022/05/space-force-adding-new-cyber-squads-improving-satellite-control/.

281 Chris Gordon, "Cybersecurity Is the 'Soft Underbelly' of Space Operations, SpOC Commander Says," *Air & Space Forces Magazine*, October 14, 2022, https://www.airandspaceforces.com/cybersecurity-is-the-soft-underbelly-of-space-operations-spoc-commander-says/.

The USSF also has created four new Space Force service components to support regional combatant commands in South Korea, the Middle East, Europe, and the Pacific.[282]

Members of Congress have been discussing creating a Space National Guard as a reserve component for the USSF to tap into the expertise at the state level: about 1000 Air National Guard members support USSF operations.[283] The 2024 defense authorization bill requires the Secretary of Defense to submit a study to Congress in March 2024 about various options for doing so.[284] In January 2024, a bill was introduced in the Senate to create a Space National Guard, something the White House has opposed due to concerns about creating "new bureaucracy with far-reaching and enduring implications and expense."[285] This bill had also been introduced in 2022 and 2023.[286]

In January 2024, the US Army released a memo to give guidance for how it can use space to support multidomain operations (MDO), which calls for it to be able to integrate capabilities in support of Army warfighting functions (to include PNT, force tracking, environmental monitoring, space domain awareness, and geospatial information), as well as the need to be able to "interdict adversary space capabilities by delivering necessary fires and effects to protect friendly forces from observation and targeting by counter-satellite communications, counter-surveillance and reconnaissance, and navigation warfare operations."[287]

US Counterspace Budget and Exercises

Despite this increased rhetoric, the unclassified US national security space budget contains a relatively small amount of funding for dedicated counterspace programs (excluding SSA) but has seen recent increases. Between FY2016 and FY2017, the total unclassified research, development, testing, and evaluation (RDT&E) budget for counterspace programs increased from $24.1 million to $41.9 million,[288] and it increased again in FY2018 to $68.38 million.[289] Nearly all of the increase was to support the development of the 10.3 version of the CCS electronic warfare system. The FY2018 budget also included $28.8 million to purchase two new 10.2 versions of CCS for active-duty USAF and Air National Guard units.[290] The FY2019 budget for these same programs decreased to $26.7 million.[291] 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.[292]

In March 2019, the Pentagon released its FY2020 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 percent in requested funding for military space programs, space control and counterspace programs saw a 46 percent decrease in requested funding.[293] 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 continued at modest funding levels.[294] In February 2020, the Pentagon released its FY2021 budget request, which included an increase of 36 percent in funding for counterspace programs, mainly due to accelerating the development of additional CCS systems. The Pentagon also asked for $77 million in overseas contingency operations funding to support counterspace operations.[295] The DoD budget request released in April 2022 asked for $63 million for counterspace systems in FY2023 as part of its procurement budget line, increasing to $67 million in FY2024, and then dropping considerably to $4 million in FY2025 and eventually $2 million in FY2027.[296] $60 million was eventually appropriated

282 Theresa Hitchens, "Space Force takes first step to establish components in commands from Europe to Asia," *Breaking Defense*, November 29, 2021, https://breakingdefense.com/2021/11/space-force-takes-first-step-to-establish-components-in-commands-from-europe-to-asia/.

283 Svetlana Shkolnikova, "Lawmakers Again Seeking Creation of Space National Guard," *Stars & Stripes*, February 14, 2024, https://www.stripes.com/branches/space_force/2024-02-14/space-national-guard-legislation-senators-13004467.html.

284 ISandra Erwin, "National Guard, Air Force, working to resolve impasse over space units," *SpaceNews*, February 8, 2024, https://spacenews.com/national-guard-air-force-working-to-resolve-impasse-over-space-units/.

285 Shkolnikova, "Lawmakers Again Seeking Creation of Space National Guard," ibid.

286 Erwin, "National Guard, Air Force, working to resolve impasse over space units," ibid.

287 Army Space Vision Supporting Multidomain Operations, U.S. Army, January 8, 2024, https://www.smdc.army.mil/Portals/38/Documents/Army_Space_Vision_Supporting_MDO.pdf.

288 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.

289 Ibid, p. 697.

290 Ibid, p. 697.

291 Ibid, p. 751.

292 *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.

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

294 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.

295 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/.

296 LI CTRSPC - Counterspace Systems, Budget Justifications FY2023 Air Force, Procurement: Space Force, April 2022, vol. 1-11, https://www.saffm.hq.af.mil/Portals/84/documents/FY23/PROCUREMENT_/FY23%20Space%20Force%20Procurement.pdf?ver=vMyfar1xW31ifPH-Fc-mz6A%3d%3d.

for it in FY 2023.[297] RDT&E for the Space Force included $58 million for space control programs and anticipated increases every year through FY2027, when the annual request is planned to be for $63 million.[298] The final amount appropriated in FY2023 for space control technology was $50 million.[299] The FY2024 request for procurement of the CCS system as part of the USSF's counterspace program element was $53 million, then dropping to $2 million for the next three fiscal years.[300]

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 most recent version was held in March 2023; this 16th iteration of this wargame had 350 participants from seven countries, 14 commercial service providers, and 25 US government commands and agencies.[301] 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.[302] The 13th Space Flag (Space Flag 22-1) was held in December 2021 and was the third Space Flag that included partners like Australia, the United Kingdom, and Canada.[303] Space Flag 22-3 was held in August 2022 and included for the first time the 5th Electronic Warfare Squadron; it was followed in December 2022 by Space Flag 23-1, which included US Army space operations officers and members from the Australian, Canadian, and UK militaries.[304] 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.[305] In July 2023, USSOUTHCOM held its first defensive space control operation during Resolute Sentinel 23, where forces from the region and USSOUTHCOM responded to electromagnetic interference as part of the Operation Thundergun Express exercise.[306]

297 "FY2023 Final Appropriations Mission Profiles," Velos, December 22, 2022, https://files.constantcontact.com/bd3dd1d9401/c741b650-75a0-4e84-9518-88578318935b.pdf?rdr=true.

298 PE 1206438SF / Space Control Technology, Budget Justifications FY 2023 Research, Development, Test & Evaluation, Space Force, April 2022, vol. 1-155, https://www.saffm.hq.af.mil/Portals/84/documents/FY23/RDTE_/FY23%20Space%20Force%20Research%20Development%20Test%20and%20Evaluation.pdf?ver=I2npdFjyjdbiZU_fpVnOAw%3d%3d.

299 "FY2023 Final Appropriations Mission Profiles," Velos, December 22, 2022, https://files.constantcontact.com/bd3dd1d9401/c741b650-75a0-4e84-9518-88578318935b.pdf?rdr=true.

300 Program Elements for Code B Items: 1206421SF, 3022F: Procurement, Space Force / BA 01: Space Procurement, SF / BSA 10: Space Programs, CTRSPC / Counterspace Systems, USSF, March 2023, vo.l. 1-7, https://www.saffm.hq.af.mil/Portals/84/documents/FY24/Procurement/FY24%20Space%20Force%20Procurement.pdf?ver=ewSd5VeJkGwWEzaSq_cd_Q%3d%3d.

301 "Schriever Wargame 2023 concludes," Space Training and Readiness Command Public Affairs, April 3, 2023, https://www.starcom.spaceforce.mil/News/Article-Display/Article/3350385/schriever-wargame-2023-concludes/.

302 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/.

303 Mike Stone, "U.S. Space Force holds war game to test satellite network under attack," Reuters, December 13, 2021, https://www.reuters.com/business/aerospace-defense/us-space-force-holds-war-game-test-satellite-network-under-attack-2021-12-14/.

304 "STARCOM executes first JNTC-accredited, largest SPACE FLAG exercise ever," Space Training and Readiness Command Public Affairs / August 22, 2022, https://www.spaceforce.mil/News/Article/3135368/starcom-executes-first-jntc-accredited-largest-space-flag-exercise-ever/; Jason Cutshaw, "Army space professionals participate in exercise Space Flag," U.S. Army public affairs, December 28, 2022, https://www.army.mil/article/263011/army_space_professionals_participate_in_exercise_space_flag.

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

306 Jennifer Whitaker, "RS23 Space Team ACEs Space Deployment," Air Forces (Southern) Public Affairs, July 18, 2023, https://www.southcom.mil/MEDIA/NEWS-ARTICLES/Article/3464169/rs23-space-team-aces-space-deployment/.

55.7558°N

02

RUSSIA

37.6173°E

Over the last two decades, Russia has renewed efforts to regain 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, and sometimes exceeded, the United States in many areas. While often not quite as technologically advanced as their US 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, like destroying critical US military satellites or countering 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 offensive counterspace capabilities. In some cases, the evidence suggests legacy capabilities are being brought out of mothballs, and in other cases, the evidence points to new capabilities being developed such as the Nudol DA-ASAT. 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-destructive counterspace capabilities in current military conflicts. There are multiple, credible reports of Russia using jamming and other electronic warfare measures in Syria and Ukraine, as well as cyber counterspace weapons, and there are indications that these capabilities are tightly integrated into Russian military operations in other regions as well.

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 /
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 match 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.

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

Specifics /

During the Cold War, the Soviet Union had multiple efforts to develop, test, and deploy co-orbital ASAT capabilities. Many different concepts for the 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. Kinetic 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.[1] 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 Imagery Appendix, pg. 16-10). 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. Many of the events are described in detail in the NASA History of On-orbit Satellite Fragmentations.[2]

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, with the system being declared operational in February 1973.[3]

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

2 J.-C. Liou, "History of On-Orbit satellite Fragmentations," NASA Orbital Debris Program Office, 15th Edition, July 4, 2018, https://ntrs.nasa.gov/api/citations/20180008451/downloads/20180008451.pdf.

3 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 2-1 — IS TESTS CONDUCTED BY THE SOVIET UNION [4]

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)	Attacked twice: by Cosmos 374 on Oct. 23 and by Cosmos 375 on Oct. 30
Feb. 25, 1971	Cosmos 394	Cosmos 397 (IS)	Successful intercept, debris created
Mar. 18, 1971	Cosmos 400	Cosmos 404 (IS)	Longer test flight with new approach from above to intercept target
Dec. 3, 1971	Cosmos 459	Cosmos 462 (IS)	Successful intercept, debris created
Feb. 16, 1976	Cosmos 803	Cosmos 804, Cosmos 814 (IS)	Attacked twice: by Cosmos 803 on Feb. 12 and by Cosmos 804 on Feb. 16
July 9, 1976	Cosmos 839	Cosmos 843 (IS)	Intercepted satellite, but possible failure
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-M)	Successful intercept, debris created
Apr. 18, 1980	Cosmos 1171	Cosmos 1174 (IS-M)	Unsuccessful intercept, debris created
Feb. 2, 1981	Cosmos 1241	Cosmos 1243, Cosmos 1258 (IS-M)	Attacked twice: Cosmos 1243 on Feb. 2 and Cosmos 1258 on Mar. 14 (both failures)
June 18, 1982	Cosmos 1375	Cosmos 1379 (IS-PM)	Successful intercept, debris created

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

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.[5] IS-M was allegedly capable of targeting satellites at altitudes of up to 2,200 km, and inclinations of 50 to 130 degrees, with an estimated kill probability of 70–80 percent.[6] IS-M also reduced attack time by increasing speed and maneuverability to allow rendezvous with the target in a single orbit.[7] The final test of the IS-M system occurred in 1982; in 1983, a moratorium was declared on all ASAT tests,[8] 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 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.

Almaz Space Station

During the 1970s, the Soviet Union developed a series of classified military space stations known as the Almaz program ("diamond" in Russian). The program began in the 1960s, before the civil and publicly-known Salyut space station program, and was a response to the American Manned Orbiting Laboratory (MOL) program.[9] The concept was to use crewed space stations to conduct military missions such as imagery and reconnaissance that was not possible by robotic satellites at that time. Three Almaz space stations flew between 1973 and 1975 under the official/cover names of OPS-1/Salyut 2, OPS-2/Salyut 3, and OPS-3/Salyut 5.

Two of the three Almaz space stations - Salyut 2 and Salyut 3 - carried weapon systems that were purportedly for "defensive" purposes but could be used offensively in certain situations.[10] The main weapon system was the R-23 Kartech, a modified 23 mm tailgun from a Tu-22 bomber that was mounted on the forward belly of the station.[11] The cannon was reportedly only test-fired once at the end of OPS-1/Salyut-3 and had significant limitations. As the cannon was fixed to the station, the entire station needed to be re-orientated to aim it, and due to orbital mechanics likely only had a relatively short range.

The cannon was slated to be replaced by a more advanced missile system starting with the OPS-4 space station but never did, as the program was canceled. The missile system was known as "Shield-2" and would have been a radar-guided missile capable of hitting another space object up to 100 km (60 miles) away.[12] The Shield-2 system reportedly used a series of small solid rocket charges to propel itself, which could also be detonated in close proximity to the target to create shrapnel.

5 Ibid.

6 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.

7 Laura Grego, "Á History of Anti-Satellite Programs," *Union of Concerned Scientists*, January 2012, https://www.ucsusa.org/sites/default/files/legacy/assets/documents/nwgs/a-history-of-ASAT-programs_lo-res.pdf.

8 Grego, ibid, p. 5.

9 Anatoly Zak, "Origin of the Almaz project," *Russian Space Web*, http://www.russianspaceweb.com/almaz_origin.html, accessed February 17, 2022.

10 Bart Hendrickx and Dwayne A. Day, "Diamonds and DORIANS: program troubles, operations, cancellation, and legacy (part 3)," *The Space Review*, January 2, 2024, https://www.thespacereview.com/article/4717/1.

11 Anatoly Zak, "Here Is the Soviet Union's Secret Space Cannon," *Popular Mechanics*, November 16, 2015, https://www.popularmechanics.com/military/weapons/a18187/here-is-the-soviet-unions-secret-space-cannon/.

12 Anatoly Zak, "Soviet space rocket-propelled grenade revealed." *Russian Space Web*, http://russianspaceweb.com/almaz-shield2.html, accessed February 17, 2022.

Naryad

Towards the end of the Cold War, the Soviet Union began developing 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,[13] 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.[14]

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

Table 2-2 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.[15] A third orbital flight test from Baikonur was conducted in December 1994, with a Rockot booster delivering the Radio ROSTO amateur radio satellite (1994-085A, 23439) into a 1,900 by 2,145 km orbit.[16] It is rumored that the launch had a second payload, which may have been the Naryad interceptor, that fragmented shortly after launch. Twenty-seven pieces of orbital space debris were cataloged, of which 24 are still on orbit along with the ROSTO satellite.

TABLE 2-2 — SUSPECTED NARYAD FLIGHT TESTS

DATE	BOOSTER	PAYLOAD	LAUNCH SITE	LAUNCH PAD	ORBIT
Nov. 20, 1990	Rockot/Briz-K	Naryad-V anti-satellite	Baikonur	Site 131	Sub-orbital
Dec. 20, 1991	Rockot/Briz-K	Experimental, Naryad test?	Baikonur	Site 175/1	Sub-orbital
Dec. 26, 1994	Rockot/Briz-K	Radio-ROSTO, Naryad test?	Baikonur	Site 175/1	1,900 km; 65°

After the fall of the Soviet Union, the components of the Naryad program found new commercial uses, leading to speculation that the program could be revived. The rocket has become the Rockot commercial launch vehicle operating from Plesetsk Cosmodrome (see Imagery Appendix, pg. 16-06), which has had 28 successful launches and placed more than 70 satellites into orbit.[17] The Naryad upper stage was developed into the Briz-KM and Briz-M, which are mainstays of Russian space launches to GEO.[18] 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.[19] It remains unclear precisely what those designations refer to, or what the difference between the two subsystems 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 after periods of dormancy.

13 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.

14 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.

15 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.

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

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

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

19 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/.

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

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.[20] 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 afterward 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, the US 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.[21]

From launch through the end of 2019, Cosmos 2491 did not make any significant changes to its orbit and remained at a relatively high LEO altitude of 1,500 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 51 pieces of orbital debris that were eventually cataloged by the US military.[22] 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. As of February 2024, Cosmos 2491 is still in a high LEO orbit of close to 1,500 km altitude.

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.[23] The process took several months, and it was not until the end of November when Cosmos 2499 passed within a kilometer of the Briz-KM.[24] 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.[25] After drifting apart, Cosmos 2499 did another series of maneuvers in January 2015 to put itself in an orbit that kept it a few km above and several hundred km 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 km per day.

Since 2016, Cosmos 2499 appears to have reached end-of-mission, but has experienced two additional events. On October 23, 2021, Cosmos 2499 experienced a fragmentation event and another on January 4, 2023, releasing a total of 59 cataloged fragments. The most likely cause of these incidents is rupture of an onboard fuel tank or some other anomaly, and given that Cosmos 2491 also experienced a fragmentation event in 2019, this suggests a potential design flaw in the 14F153 satellite series. As of February 2024, Cosmos 2499 is still in orbit but inactive.

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

20 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.

21 Jonathan McDowell, "Jonathan's Space Report No. 697," May 17, 2014, https://planet4589.org/space/jsr/back/news.697.txt.

22 Jonathan McDowell, Tweet, 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.

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

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

25 Пашков, Дмитрий, "Cosmos-2491/RS-46 (R4UAB)," Youtube, December 2, 2014, https://www.youtube.com/watch?v=jHKoSdhM-VDk#t=14. The Russian government publicly disclosed the existence of the amateur radio payloads, which were activated at the end of the main mission.

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 six 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 its 2007 ASAT test.[26] 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.[27] As of February 2024, Cosmos 2504 was still in orbit but inactive.

On June 23, 2017, a Russian Soyuz 2-1v rocket was launched from Plesetsk (see Imagery Appendix, pg. 16-07) 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.[28] 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).[29] 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.[30] 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."[31] Subsequently, Russia reported that the satellite-inspector completed a series of proximity operations experiments and returned to the Cosmos 2519 host satellite on October 26.[32] 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.[33] Jonathan McDowell calculated that Cosmos 2523 was released at a relative velocity of 27 meters per second (60 miles per hour).[34] Comments from senior US military leadership suggest they consider the deployment of Cosmos 2523 to have been an ASAT test, given its relatively large deployment velocity.[35] Throughout March, April, and June 2018, Cosmos 2519 and 2521 conducted several RPOs of each other.[36] Since 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.[37] Cosmos 2521 eventually re-entered the atmosphere on September 12, 2019[38] and Cosmos 2519 re-entered on December 23, 2021.[39] As of February 2024, Cosmos 2523 remains in orbit.

Links to Project Nvelir and Burevestnik

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.[40] Publicly-available documents and patents suggest a link between those Cosmos satellites and

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

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

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

29 "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.

30 Bart Hendrickx, posting on the NASAspace-flight.com Forums, February 27, 2018, https://forum.nasaspaceflight.com/index.php?PHPSESSID=35dsgsej5k8t-t51h7fo7re8e04&topic=43064.ms-g1793720#msg1793720.

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

32 Jonathan McDowell, "Jonathan's Space Report No. 742," November 25, 2017, https://planet4589.org/space/jsr/back/news.742.txt.

33 Bart Hendrickx, posting on the NA-SAspaceflight.com forums, March 3, 2018, https://forum.nasaspaceflight.com/index.php?topic=43064.msg1795369#msg1795369.

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

35 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/.

36 Jonathan McDowell, "Jonathan's Space Report No. 752," August 17, 2018 https://planet4589.org/space/jsr/back/news.752.txt.

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

38 "The United States Reported that Russia Lost a Military Satellite Inspector," *TASS*, September 13, 2019, https://tass.ru/kos-mos/6882787.

39 "Russian military satellite that worked with inspector spacecraft burns in atmosphere," *TASS*, December 23, 2021, https://tass.com/science/1380133.

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

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).[41] 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.[42] Burevestnik appears to involve ground-based infrastructure at Plesetsk Cosmodrome near Noginsk-9 (see Imagery Appendix, pg. 16-08), 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. Additional reports suggest Burevestnik includes a three-stage solid fuel rocket built by NPO Iskra.[43] It appears this rocket is intended to be launched from a modified MiG-31 fighter aircraft (labeled MiG-31BM) to serve as a quick-response system to place the Burevestnik ASATs into orbit. The concept is a new version of the Ishim proposal from the early 2000s and using a fighter as a launch platform would enable significant flexibility for launch times and orbits to target.[44]

FIGURE 2-1 — MiG-31BM CARRYING A BUREVESTNIK LAUNCHER

Credit: ShipSash

The Nivelir inspection and Buresvestik co-orbital ASAT programs share a lot of technologies. They 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.[45] 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).[46] 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.[47] Another possibility is that the interceptors might use explosive charges to generate fragments, as indicated by a contract given to the Krasnoarmeysk Scientific Research Institute of Mechanization (KNIIM) and a company called OOO Expotekhvzryv as part of Burevestnik.[48]

Another Rodnik replenishment mission was launched from Plesetsk on

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

42 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.

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

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

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

46 Ibid.

47 Ibid.

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

November 30, 2018, and 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 a dummy payload that replaced a laser reflector satellite at the last minute.[49] 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 (see Imagery Appendix, pg. 16-07), designated by the US military as Cosmos 2535 (2019-039A, 44421), Cosmos 2536 (2019-039B, 44422), Cosmos 2537 (2019-039C, 44423), and Cosmos 2538 (2019-039D, 44424). All four objects were registered with the United Nations in August 2019.[50] 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.[51] 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.[52] According to data compiled by Jonathan McDowell, the two satellites conducted a series of RPO experiments between August 7 and 19, 2019, with approach distances as close as 30 km before backing off to 180 to 400 km.[53] Shortly before the RPO, nine debris objects were released in the vicinity of the two satellites, with apogees as high as 1,400 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, has 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, 30 cataloged debris objects have been associated with this launch as of February 2021.[54] As of February 2024, Cosmos 2535 and 2536 are still on orbit but inactive.

On November 25, 2019, Russia conducted another launch of a Soyuz-2-1v from Plesetsk (see Imagery Appendix, pg. 16-7) with an announced military payload on board. The satellite was cataloged by the US military as Cosmos 2542 (2019-079A, 44797) in a 97.9° inclination and 370 by 860 km orbit. The mission of the satellite as announced by Russia was to conduct space surveillance as well as Earth remote sensing.[55] Outside experts have indicated it is likely the second satellite in the Nivelir 14F150 series.[56] On December 6, Cosmos 2542 released a small subsatellite that was cataloged by the US military as Cosmos 2543 (2019-079D, 44835) and publicly announced by Russia.[57] 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.[58] 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 US 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.[59]

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

50 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.

51 Cees Bassa, Twitter, July 12, 2019, https://twitter.com/cgbassa/status/1149662117819060224.

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

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

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

55 "Успешный пуск ракеты-носителя «Союз-2.1в»", *TASS*, November 26, 2019, https://www.roscosmos.ru/27793/.

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

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

58 Jonathan McDowell, "Space Activities in 2019," January 12, 2020, p. 29, https://planet4589.org/space/papers/space19.pdf.

59 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.

The close proximity of Cosmos 2543 to USA 245 sparked concerns from the US military. General 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 US military considers to be a weapons test.[60] 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.[61]

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.[62] And in late April, Cosmos 2542 lowered its perigee to increase the separation and create a gradual separation in planes between the two satellites.[63] Cosmos 2542 was decommissioned in May 2023 and re-entered the atmosphere on October 24, 2023.

In June 2020, Cosmos 2543 made a series of maneuvers to place it into RPO with Cosmos 2535, including close approaches within 60 kilometers.[64] 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.[65] 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).[66] The US 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. Jonathan McDowell noted that the release occurred while the objects passed over Plesetsk.[67] 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."[68] The head of the United Kingdom's Space Directorate, Air Vice Marshal Harvey Smyth, also released a public statement on Twitter expressing concerns and calling on Russia to avoid further testing.[69] 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.[70]

60 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/.

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

62 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.

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

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

65 "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.

66 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.

67 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.

68 USSPACECOM Public Affairs Office, "Russia conducts space-based anti-satellite weapons test," *United States Space Command*, July 23, 2020, https://www.spacecom.mil/Newsroom/News/Article-Display/Article/2285098/russia-conducts-space-based-anti-satellite-weapons-test/.

69 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.

70 "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.

Cosmos 2535 and Cosmos 2543 remained in close proximity through August 2020, and by August 13, they were joined by Cosmos 2536.[71] In late September 2020, Cosmos 2535 and Cosmos 2536 were close enough that they are presumed to have docked.[72] In mid-October, Cosmos 2536 separated away from Cosmos 2535 to a distance of 20 kilometers.[73] As of February 2024, both objects are still in orbit but slowly decaying.

On August 1, 2022, another Russian Soyuz 2.1v launch vehicle from Plesetsk (see Imagery Appendix, pg. 16-07) placed a mysterious satellite, dubbed Cosmos 2558 (2022-089A, 53323) into LEO. The launch timing and initial orbit appeared to coincide with the orbital plane of USA 326, a classified NRO imagery satellite that was launched in February 2022. Analysis suggested that the orbits of Cosmos 2558 and USA 326 were very similar in inclination and would periodically come within 60 to 70 km in altitude.[74] On August 18, 2022, USSPACECOM released a statement condemning Russia for this behavior, calling the activities of Cosmos 2558 "dangerous and irresponsible behavior."[75] Further analysis confirmed that as of September 2022 Cosmos 2558 had altered its orbit to continue to match the orbital plane of USA 326, although it is not in an actual proximity orbit.[76] Cosmos 2558 and USA 326 appear to have been in similar orbits through at least April 2023.[77] It is unclear whether Cosmos 2558 is related to Cosmos 2535 or Cosmos 2542.

On December 1, 2022, a Soyuz 2.1b launched from Plesetsk placed Cosmos 2565 (2022-163A, 54381) into a 900 km by 239 km at 67.15 degree LEO.[78] Cosmos 2565 is believed to be an electronic intelligence satellite in the Lotos-S1 series, given its orbit matching previous satellites in that constellation. Two days later, Cosmos 2565 had raised its orbit to 912 km by 899 km and released a small satellite, Cosmos 2566 (2022-163C, 54383). In late December a third object, labeled Object D (2022-163D, 54817) was released from Cosmos 2566. On October 27, 2023, another Soyuz 2.1b from Plesetsk placed Cosmos 2570 (2023-165A, 58148), believed to be another in the Lotos series, into a similar orbital profile. It also released another satellite, Cosmos 2571 (2023-165B, 58172), after circularizing, which once again released a third satellite, cataloged as Object D (2023-165C, 58428) in late November. Commercial satellite tracking firm LeoLabs reported that Object D had maneuvered and performed at least one close pass of Cosmos 2571, potentially as part of an imaging attempt.[79] However, the activities of these sets of satellites do not appear to constitute sustained RPO, and the deployment of their sub satellites is substantially different than that of Cosmos 2523.

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."[80] Russian filings with the United Nations reference the satellite as "Luch,"[81] 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.

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

72 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.

73 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.

74 Marco Langbroek, "Kosmos 2558, a Russian inspector satellite targeting the US IMINT satellite USA 326?," SatTrackCam Leiden (b)log, August 2, 2022, https://sattrackcam.blogspot.com/2022/08/kosmos-2558-russian-inspector-satellite.html.

75 Brett Tingley, "Pentagon space chief condemns "irresponsible' launch of Russian inspector satellite," Space.com, August 18, 2022, https://www.space.com/russia-inspector-satellite-kosmos-2558-irresponsible-behavior.

76 Marco Langbroek, "Kosmos 2558 keeping its orbit close to USA 326," SatTrackCam Leiden (b)log, September 9, 2022, https://sattrackcam.blogspot.com/2022/09/kosmos-2558-keeping-its-orbit-close-to.html.

77 Scott Tilley (@coastal8049), "Nico Janssen noted that the NRO Keyhole USA 326 pursued by COSMOS 2558 had changed it's orbit. We know that historically that KH satellites will typically use their S-band transmitters around orbital changes so I looked for it today and it appears I was rewarded!" posting on X, April 9, 2023, https://x.com/coastal8049/status/1645197516395397120?s=20.

78 Anatoly Zak, "Soyuz launches military payload," *Russian Space Web*, November 25, 2023, https://www.russianspaceweb.com/lotos-s1-807.html.

79 Theresa Hitchens, "LeoLabs: Russia, China time suspicious satellite activity for some US holidays," BreakingDefense, December 12, 2023, https://breakingdefense.com/2023/12/leolabs-russia-china-time-suspicious-space-activity-for-some-us-holidays/.

80 Anatoly Zak, "Proton Successfully Returns to Flight Delivering a Secret Olymp Satellite," *Russian Space Web*, October 19, 2015, http://www.russianspaceweb.com/olymp.html.

81 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=ST/SG/SER.E/761.

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 relatively 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.[82] 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 satellite.[83] During its nearly decade on orbit, Luch has parked near more than two dozen commercial communications satellites for periods ranging from a few weeks to nine months,[84] and typically close enough to be within the typical ground terminal uplink window.[85] The closest known approach was with 1.8 km of Intelsat 36.[86] The orbital history of Luch is documented in Figure 2-2.

82 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/.

83 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.

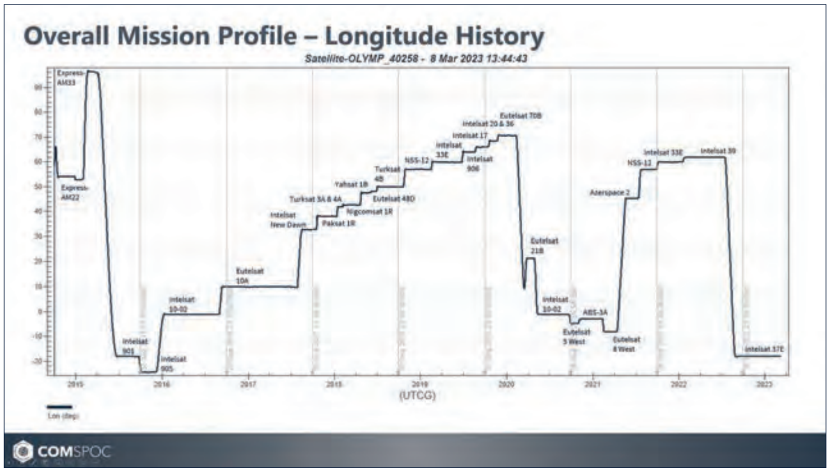
84 Marco Langbroek, “LUCH (Olymp-K), an eavesdropping SIGINT snooping around commercial comsats,” *SatTrackCam Leiden (b)log*, April 6, 2021, https://sattrackcam.blogspot.com/2021/04/luch-olymp-k.html/.

85 Bob Hall, “Luch Space Activities,” *AGI web series*, Ep. 14, June 26, 2019, https://youtu.be/D67dg9P3eDY.

86 Ibid.

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

FIGURE 2-2 — LUCH (OLYMP) ORBITAL HISTORY



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

Open source research has revealed more details about the originals of the Luch Olymp program. The ground-based RF tracking firm Kratos conducted an analysis of the activities of both Luch Olymp satellites and concluded they are likely being used for a signals intelligence mission, which is done by parking close enough to a target satellite to collect RF signals uplinked to it.[87] This conclusion is corroborated by sources from within the Russian space agency who have stated that the satellite is called Olimp and had been ordered by the Federal Security Service (FSB) for a signals intelligence mission, which it accomplishes by parking close enough to a target satellite to intercept up-linked radiofrequency signals.[88]

On March 12, 2023, a Russian Proton-M rocket from Baikonur Cosmodrome placed another satellite in GEO that has since behaved very similar to Luch.[89] This new satellite, cataloged as Luch Olymp 2 (2023-031A, 55841), and designated Luch 5X in registration filings with the United Nations, appears to have resumed the RPO activities of the original Luch. It was was briefly near the Russian military satellite Cosmos 2533 (2018-107A, 43867) near 70 degrees east longitude on March 18 and the US Space Force's WGS F2 (2009-17A, 34713) military communications satellite near 60 degrees east longitude from April 7 to May 5. It has since spent much longer periods of time next to Eutelsat 9B (2016-005A, 41310) and Eutelsat KA-SAT 9A (2010-069A, 37258) at 9 degrees east longitude from May 20 until September 23, Eutelsat 3B (2014-030A, 39773) from October 7 to December 5, and Eutelsat Konnect VHTS (2022-110A, 53765) at 2.7 degrees east from December 6 until the time of publication.[90] The orbital history of Luch 2 is documented in Figure 2-3.

87 Michael Clonts, "Espionage in Orbit: Satellite or Spy?," *Kratos*, April 17, 2023, https://www.kratosdefense.com/constellations/articles/espionage-in-orbit-satellite-or-spy.

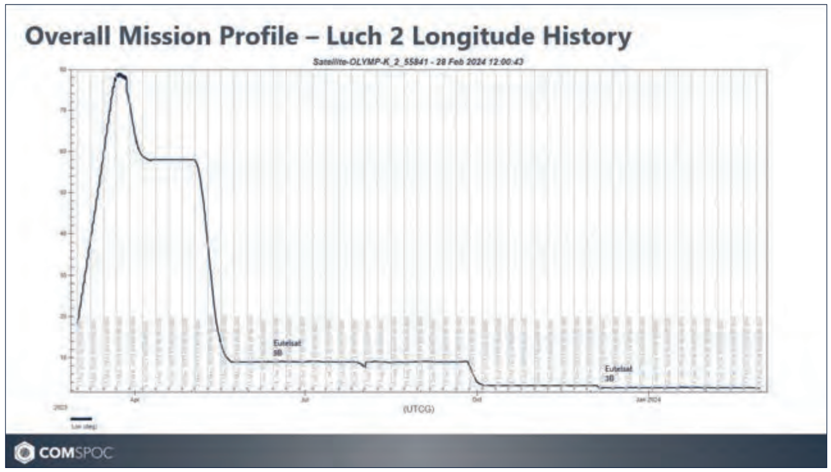
88 Bart Hendrickx, "Olimp and Yenisi-2: Russia's secretive eavesdropping satellites (part 1)," *The Space Review*, November 20, 2023, https://www.thespacereview.com/article/4696/1.

89 Justin Mooney, "Russian Proton-M launches Olymp-K-2 military satellite," Nasaspaceflight.com, March 12, 2023, https://www.nasaspaceflight.com/2023/03/proton-olymp-k-2/.

90 Brian Weeden, "Our Satellite Dashboard shows this new Luch hung out near the Space Force WGS F2 near 60E from April 7 to May 5, then the Eutelsat 9A/9B/10A at 9E and 10E from May 20 until Sept 23, at times coming well within 10 km", posting on X, October 4, 2023, https://twitter.com/brianweeden/status/1709622408288543076.

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

FIGURE 2-3 — LUCH 2 ORBITAL HISTORY



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

All the recent Russian RPO activities in LEO and GEO are summarized in Table 2-3.

TABLE 2-3 — RECENT RUSSIAN RPO

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 a 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. 2023	Luch, (Olymp), Multiple	35,600 km, 0°	Luch parked near more than two dozen communications satellites over nearly a decade, including those owned by Russia, the United States, Pakistan, Turkey, the United Arab Emirates, France, and Italy.
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 do inspections before redocking with Cosmos 2519. 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.
Aug. – Dec. 2019	Cosmos 2535, Cosmos 2536	623 x 621 km; 97.88°	Cosmos 2535 and Cosmos 2536 conducted at least 25 individual RPO operations to within 2 km and as far apart as 380 km.
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.

DATE(S)	SYSTEM(S)	ORBITAL PARAMETERS	NOTES
Nov. 2022	Cosmos 2562, Resurs-P3	400 x 385 km; 97.2°	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.
Mar. 2023 - Current	Luch (Olymp) 2, Multiple	35,600 km, 0°	Luch 2 has parked next to multiple American and European communications satellites.

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.[90] 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.[92] Such a payload could have significant benefits for RPO and co-orbital ASAT weapons. On October 21, 2022, Russia launched two satellites, Cosmos 2561 (2022-137A, 54109) and Cosmos 2562 (2022-137B, 54110), into LEO on a Soyuz-2.1v rocket. Initial analysis suggests they are two new types of satellites (designated 14F164 and 14F172) and may be part of the Numizmat program.[93] On November 15, 2022, a formerly inactive Russian Earth observation satellite, Resurs-P3 (2016-016A, 41386), performed a large maneuver to drop its orbit by 20 km, and on November 22, Cosmos 2562 maneuvered to conduct an RPO of Resurs-P3. US commercial SSA company LeoLabs assessed Cosmos 2562 as highly likely to have an electro-optical payload [that] collected high-resolution imagery of Resurs-P3.[94] This suggests Cosmos 2562 was attempting to inspect Resurs-P3 to diagnose the anomaly that led to its initial failure. Cosmos 2562 subsequently re-entered the atmosphere on November 8, 2023.

Potential Nuclear Co-Orbital Weapon

In February 2024, rumors emerged about the existence of a new kind of Russian co-orbital ASAT threat. It began on February 15 with a cryptic public announcement from Representative Mike Turner, Chairman of the House Select Permanent Committee on Intelligence, that his committee was making classified intelligence on a new Russian threat available to all members of Congress.[95] The following day, anonymous government sources clarified that the threat in question had to do with a new Russian program to develop a "space-based capability to attack satellites using a nuclear weapon."[96] The Biden administration also clarified that this capability is still in development and not yet deployed in orbit, but if done so it would constitute a breach of the Outer Space Treaty, which aligns with a nuclear weapon placed into orbit.[97] Although details still remain scarce, it appears the capability in question would utilize a nuclear weapon to generate an electromagnetic pulse (EMP) that could damage or disable large swaths of satellites.

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, surveillance and intelligence collection. 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 US RPO missions to test and demonstrate satellite inspection and servicing capabilities, in particular, XSS-11 and Orbital Express (see US Co-Orbital ASAT,

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

92 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.

93 Bart Hendrickx, "Re: Soyuz-2.1v/Volga - Kosmos 2561/2562 - Plesetsk 43/4 - 21 Oct 2022 19:20 UTC," NASASpaceflightForums.com, January 9, 2023, https://forum.nasaspaceflight.com/index.php?topic=57374.msg2447737#msg2447737.

94 Sandra Erwin "LeoLabs data shows on-orbit maneuvers by Russian satellites," *SpaceNews*, November 6, 2023, https://spacenews.com/leolabs-data-shows-on-orbit-maneuvers-by-russian-satellites/.

95 House Intelligence Committee, "Statement from Chairman @RepMikeTurner," posting on X, February 15, 2024, https://x.com/HouseIntel/status/1757805804885823775?s=20.

96 Christian Davenport, Ellen Nakashima, Abigail Hauslohner, and Shane Harris, "With a dire warning, concerns rise about conflict in space with Russia," The Washington Post, February 15, 2024, https://www.washingtonpost.com/technology/2024/02/15/space-weapons-russia-china-starlink/.

97 Dustin Volz and Gordon Lubold, "White House confirms Russia is developing antisatellite weapons," *The Wall Street Journal*, February 15, 2024, https://www.wsj.com/politics/national-security/russia-space-weapon-classified-confirmed-b5beacf.

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

Section 1.1). Such inspection or surveillance could be used to support target identification and tracking for attacks by other counterspace capabilities.

The on-orbit behavior of both Luch satellites strongly suggest a signals intelligence collection mission to intercept broadcasts aimed at other GEO satellites and possibly also to inspect other GEO satellites. 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 both Luchs have done. Documents from Russian industry further indicate links to a military satellite communications program, heritage to the Luch series of relay satellites, and an intelligence mission. Likely examples of the former are the activities of the US PAN satellite (35815, 2009-047A) between 2009 and 2014 (see US Co-Orbital ASAT, Section 1.1) and the Chinese SJ-17 satellite (40258, 2014-058A) in 2017 (see Chinese Co-Orbital ASAT, Section 3.1).

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 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 the 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 an ASAT interceptor deployment test, potentially linked to the Burevestnik program. The most recent activities of Cosmos 2656 and Cosmos 2570, including their deployment of multiple nested sub- satellites, appear to be substantially different from the nested subsatellite deployed by Cosmos 2019. They occurred at much lower relative velocities, suggesting they were not weapons tests and are more likely small science or possibly inspection payloads.

It may be possible to use any of these RPO satellites as a potential weapon. 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 involve 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. The military utility of a nuclear weapon used as a co-orbital EMP device is both devastating and limited. In a purely destructive sense, such a weapon could destroy large numbers of satellites. However, it would be indiscriminate and destroy Russian satellites as much as any adversary's. Some of the effects would not be felt for days, weeks, or even months as the higher radiation levels slowly degraded unhardened satellites and could persist for years afterwards, endangering the use of space by all countries. Deployment of such a weapon would also be an egregious breach of the Outer Space Treaty and likely engender swift political and diplomatic censure from a large number of countries, which would further undermine any benefit that could be derived from its use.

2.2 — RUSSIAN DIRECT-ASCENT ASAT

Assessment /

Russia has long had the potential for a DA-ASAT capability through its historical ballistic missile defense capabilities and had DA-ASAT development programs in the past that never fully became operational. In November 2021, after more than a decade of development and testing, Russia successfully demonstrated a DA-ASAT capability against a LEO satellite. It is unclear whether this system, the Nudol, will become operational soon, and it does not appear to have the capability to threaten targets beyond LEO.

Specifics /

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

1. Nudol: a current ground-launched ballistic missile that has demonstrated the ability to destroy a LEO satellite;
2. 78M6 Kontakt: a Cold-War era air-launched ballistic missile that was designed to be launched from a fighter plane and was rumored to be in active development again;
3. S-500: a next-generation exoatmospheric ballistic missile defense system, still several years from deployment, that may have capabilities against targets in low LEO orbits.

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

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 multilayered missile defense architecture.[98] 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.[99]

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.[100] The system includes the 53T6M, an upgraded version of the Gazelle, as its short-range interceptor but does not appear to have a DA-ASAT capability at this time.

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 (US designation PL-19).[101] 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.[102] Individual components were tested in 2012[103] and initial non-flight testing of the system as a whole was successfully conducted in 2013.[104] 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

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

99 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).

100 Keir Giles, "Russian Ballistic Missile Defense: Rhetoric and Reality," U.S. Army War College, June 2015, https://www.jstor.org/stable/resrep11662.

101 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.

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

103 "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.

104 GSKB Annual Report 2013.

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

105 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.

106 Bart Hendrickx, "Aerostat: a Russian long-range anti-ballistic missile system with possible counterspace capabilities," *The Space Review*, October 11, 2021, https://www.thespacereview.com/article/4262/1.

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

108 "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/.

109 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.

110 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.

111 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.

112 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/.

113 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/.

114 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.

ballistic missiles, as a subcontractor instead of OKB Novator.[105] The second contract was for a system called Aerostat, which appears to be the longer-range interceptor for the A-235 system, which is a separate program from the Nudol but still may have some DA-ASAT capability.[106]

FIGURE 2-4 — TEL-MOUNTED NUDOL

Artist's depiction from company calendar. Image credit: Almaz-Antey.[107]

The evidence suggests Nudol is being developed for the direct purpose of DA-ASAT operations. Throughout the development process, Almaz-Antey (whose role within the Russian defense complex is the development of technologies for "active space defense") has pitched the system as valuable for holding US LEO assets at risk.[108] What little is known publicly about the Nudol flight tests are more suggestive of an orbital ballistic trajectory intercept than a midcourse 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]." [109] The system appears to be designated the 14Ts033 (14Ц033), comprised of the 14A042 Nudol rocket, 14P078 command and control system, and 14TS031 radar.[110]

There have been eleven potential flight tests of Nudol, two of which were unsuccessful, eight 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.[111] A report in April 2018, citing unnamed US 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.[112] Evidence is inconclusive as to whether any of the remaining tests included a kill vehicle.[113] 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.[114] 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."[115, 116] Table 2-4 lists the known and suspected tests of the Nudol. Note that two previously listed Nudol flight tests in April and June 2021 were removed for the 2024 edition of this report, as further research indicated they had NOTAMs issued but were postponed and did not take place.

TABLE 2-4 — NUDOL FLIGHT TESTS TO DATE

DATE	SYSTEM	LAUNCH SITE	PAYLOAD	APOGEE	NOTES
Aug. 12, 2014	Nudol	?	?	X	Failed shortly after launch.
Apr. 22, 2015	Nudol	?	?	X	Failed at launch.
Nov. 18, 2015	Nudol	Plesetsk	KKV	200 km?	First successful test of missile.
May 25, 2016	Nudol	Plesetsk	??	100 km?	Appears to be likely rocket test (successful).
Dec. 16, 2016	Nudol	"Central Russia" (Plesetsk? Kapustin Yar?)	Likely KKV	100 km?	Appears to be likely rocket test (successful).
Mar. 26, 2018	Nudol	Plesetsk	Likely KKV	?	First test from a mobile launcher.
Dec. 23, 2018	Nudol	Plesetsk	Likely KKV	?	Successful PL-19 Nudol test, mobile launcher.
Nov. 15, 2019	Nudol	Plesetsk	Likely KKV	?	–
Apr. 15, 2020	Nudol	Plesetsk	Likely KKV	?	Successful, nothing hit.
Dec. 16, 2020	Nudol	Plesetsk	Likely KKV	?	Successful, nothing hit.
Apr. 2021	Nudol	Plesetsk	Likely KKV	?	Unconfirmed test.
Nov. 15, 2021	Nudol	Plesetsk	KKV	470 km	Intercepted and destroyed Cosmos 1408.

On November 15, 2021, Russia conducted the first known intercept test of the Nudol, which intercepted and destroyed Cosmos 1408 (1982-092A, 13552), a defunct Russian military satellite, at an altitude of approximately 470 km. The test was preceded by a NOTAM issued on November 13 for November 15–17 that corresponded to the usual reentry zones for a Nudol launch.[117] Cosmos 1408 passed over the launch side headed NE and the NOTAM suggests that the Nudol was launched in the same direction, meaning that it was generally traveling in the same direction as the satellite and the intercept velocity was likely lower than other DA-ASAT tests.[118] The intercept destroyed Cosmos 1408, a 1,750 kg (3,860 lb) defunct Soviet Tselina-D signals intelligence satellite,[119] and created a large amount of orbital debris. As of February 2024, more than 1,800 pieces of orbital debris larger than 10 cm (4 inches) have been cataloged from this test with 67 still in orbit.[120]

Immediately following the intercept, the Russian Foreign Ministry publicly claimed that the debris from the test "posed no threat to space activity,"[121] However, due to the proximity of the test to the orbit of the International Space Station (ISS), NASA flight directors ordered the crew onboard the ISS to take emergency shelter in the Dragon and Soyuz lifeboats.[122] The US military condemned the test, stating that it demonstrated a "deliberate disregard for the security, safety, stability, and long-term sustainability of the space domain for all nations."[123]

Little is known for sure about the operational capabilities of the Nudol, and

115 USSPACECOM Public Affairs, "Russia tests direct-ascent anti-satellite missile," *United States Space Command*, April 15, 2020, https://www.spacecom.mil/Newsroom/News/Article-Display/Article/2151611/russia-tests-direct-ascent-anti-satellite-missile/.

116 USSPACECOM Public Affairs, "Russia tests direct-ascent anti-satellite missile," *United States Space Command*, December 16, 2020, https://www.spacecom.mil/Newsroom/News/Article-Display/Article/2448334/russia-tests-direct-ascent-anti-satellite-missile/.

117 Telegram posting from Warbolts, "Еще один пуск из этой серии. Что за изделие испытывается достоверно не известно до сих пор, но эксперты связывают его с "Нудоль". Закрытия в целом повторяют ранее объявляемые, период действия 15/11/2021 02:00 (UTC) - 17/11/2021 05:00 (UTC). Из интересного, в данных NOTAM на Плесецк и Чёшскую губу указан номер телефона некоего Чирикова." November 13, 2021, https://t.me/warbolts/707.

118 Tweet from Jonathan McDowell, "Here is the pass of Kosmos-1408 (red line) northbound over Plesetsk at about 0245 UTC Nov 15. Well aligned with the NOTAM areas (indicated) for the suspected Nudol antisatellite test," November 15, 2021, https://twitter.com/planet4589/status/1460305735317868545?s=20&t=Sl7upa788x-Mw7JECDsi3og.

119 "Kosmos 1408," Wikipedia, https://en.wikipedia.org/wiki/Kosmos_1408, accessed February 16, 2022.

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

121 "New Russian system being tested hit old satellite with "goldsmith's' precision – Shoigu," *TASS*, November 16, 2021, https://tass.com/science/1362219.

122 W.J. Hennigan, "Astronauts Take Shelter Aboard ISS After Russian Anti-satellite Test, U.S. Says," *Time*, November 15, 2021, https://time.com/6117840/astronauts-shelter-iss-russia-test/.

123 U.S. Space Command Public Affairs Office, "Russian direct-ascent anti-satellite missile test creates significant, long-lasting space debris," U.S. Space Command, November 15, 2021, https://www.spacecom.mil/Newsroom/News/Article-Display/Article/2842957/russian-direct-ascent-anti-satellite-missile-test-creates-significant-long-last/.

available estimates for maximum altitude vary widely out to nearly 1,000 km.[124] The designation 14A is usually reserved for "space rockets" and intended for intercepting space objects, either satellites or nuclear warheads.[125]

The 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.[126] 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.[127] 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 US 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.[128]

It is possible that the nuclear armament of the Nudol under at least some circumstances is being considered, but the evidence is not conclusive. Available depictions of the Nudol TEL have features that appear to be environmental control systems (ECS) on the missile tubes—a feature typically associated with nuclear-armed missiles.[129] 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.[130] 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).[131] 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.[132] Moreover, Russian-language media reported in early 2018 that the system would not be equipped with nuclear warheads.[133]

124 See Jonathan McDowell, "Launch Vehicles," Accessed March 21, 2018, http://planet4589.org/space/lvdb/sdb/LV. The suspected apogees were 350 km and 500–1,000 km. 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*.

125 Ibid.

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

127 Bill Gertz, "Russia Flight Tests Anti-Satellite Missile," *The Washington Free Beacon*, May 27, 2016, http://freebeacon.com/national-security/russia-flight-tests-anti-satellite-missile.

128 U.S. Space Command Public Affairs Office,

129 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.

130 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.

131 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.

132 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.

133 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.

78M6 Kontakt

The second category of direct-ascent ASAT system explored by the Soviet Union, and potentially 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.[134] 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." [135] 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.[136] The system was also intended to be capable of deploying with little or no warning, in contrast to the USSR's co-orbital interceptors,[137] 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.[138]

The program was based out of Sary Shagan (see Imagery Appendix, pg. 16-09) with support to be provided by the Krona optical space surveillance complex, and allegedly became ready for flight-testing around 1991.[139] 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 United States from discovering the program.[140] If true, this would demonstrate the 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, there are reports that the program may have been resumed by the Russian Air Force in 2009.[141] 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.

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 Imagery Appendix; page 16-49), 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.[142] 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." [143]

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.[144] Three anonymous US government sources stated in 2018 that the system was being actively tested with the goal of reaching operational readiness in 2022; but as of February 2024, it most likely is not operational.[145] 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-31BM that would likely be used as a quick-response launch system to place one or more

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

135 Ibid.

136 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.

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

138 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.

139 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.

140 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.

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

142 "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.

143 "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.

144 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.

145 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.

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

co-orbital ASATs into orbit (see Russian Co-Orbital ASAT, Section 2.1).[146] Construction work is ongoing at Plesetsk airport to build infrastructure for future Burevestnik launches from an aircraft-carried booster and it is unclear what further role Sary Shagan will have in this program.[147]

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.[148] 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 before re-entry but also objects in orbit.[149] Russian officials, in the years following the Chinese and US ASAT and missile defense tests of the late 2000s, began to explicitly discuss the S-500 as serving a dual missile defense-ASAT purpose.[150] 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,[151] but had not yet completed testing.[152] 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.[153] Russian defense minister Sergei Shoigu announced that he expected deliveries to begin as soon as 2020, and funding has been guaranteed as part of the State Armament Program 2018–2027; [154] Russia reportedly planned to field 10 battalions of the new system.[155]

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.[156] In July 2021, Russia showed the first video footage of a containerized missile of the S-500 system being test fired from a TEL.[157] While it was reported that the first S-500 unit had been delivered to Russian forces in September 2021, Russian Deputy Prime Minister Yuri Borisov stated that it was not a mature system and still needed "configurations." [158] Even so, the S-500's manufacturer announced in April 2022 that mass production had begun and that serial delivery was intended to begin in 2025.

In December 2021, TASS reported that the S-550 system had entered service and that it was capable of "hitting spacecraft, ballistic missile reentry vehicles and hypersonic targets at altitudes of tens of thousands of kilometers." [159] However, this report was immediately called into question as other reports indicated that development of the system had not yet started or that it had been confused with the S-500.[160]

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 and 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

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

147 Bart Hendrickx, posting on NASA *Spaceflightforum.com*, July 28, 2020, https://forum.nasaspaceflight.com/index.php?topic=45734.msg2112384#msg2112384.

148 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.

149 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/.

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

151 Brendan McGarry, "Graphic Details Russian Surface to Air Missile Coverage in Europe," Military.com, August 30, 2016, https://www.military.com/defensetech/2016/08/30/detailing-russian-surface-to-air-missile-coverage-in-europe.; "S-500 Prometheus," Missile Threat, updated May 4, 2017, https://missilethreat.csis.org/defsys/s-500-prometheus/.

152 Ibid.

153 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.

154 Ibid.

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

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

157 Thomas Newdick, "This is Our First View of Russia's New S-500 Air Defense System in Action," *The Drive*, July 20, 2021, https://www.thedrive.com/the-war-zone/41627/this-is-our-first-view-of-russias-new-s-500-air-defense-system-in-action.

158 Inder Singh Bisht, "Russia Begins Mass Production of S-500 Air Defense System," *TheDefencePost*, April 28, 2022, https://www.thedefensepost.com/2022/04/28/russia-mass-producing-s-500/.

159 "First S-550 air defence systems enter service in Russia – source," *TASS*, December 28, 2021, https://tass.com/defense/1382133.

160 Joseph Trevithick, "No, Russia's S-550 Missile Defense System Hasn't Been Fielded," *The Drive*, December 29, 2021, https://www.thedrive.com/the-war-zone/43675/no-russias-s-550-missile-defense-system-hasnt-been-fielded.

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

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 2021 Nudol test. The 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. The 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 (PGMs), but has no publicly known capability to interfere with the GPS satellites themselves using radio frequency 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 current military campaigns, as well as using it within 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.[161]

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.[162]

GNSS Jamming
GNSS jamming, particularly of the US 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 is used to protect fixed facilities.

161 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/.

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

For example, Russian state media announced that Russia is deploying 250,000 GPS jammers on cell phone towers throughout the country.[163] 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 landmass, thereby protecting fixed installations. The Pole-21 systems are reported to be effective to a range of 80 km.[164]

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.[165] 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."[166] 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 PGMs. Recently, there have been multiple reports of Russia deploying some of these EW systems in support of Russian deployments in Syria and Ukraine.[167] In May 2019, the Ukrainian military released maps showing the deployment of Russian EW systems throughout the Donbas region of Ukraine.[168] Reports of GPS interference along the Ukrainian border intensified in March and April 2021.[169] In August 2021, the Jamestown Foundation released a detailed report on Russian EW activities in the Donbas region of Ukraine.[170]

In February 2022, reports of GPS interference in Ukraine spiked alongside Russia's forces entering Ukraine. Hawkeye360, a US-based commercial geospatial analytics company, said they noted increased GPS interference in and around Ukraine in the months leading up to the February attack as well as since. However, the first few months of the conflict did not include the degree of GPS interference and other kinds of electronic warfare that some analysts expected, with several different potential explanations as to why. But by July 2022, at least three of Russia's five EW brigades were reported to be involved in the fighting in Ukraine and reports of electronic warfare began to increase. GPS jamming around Russian Engles-2 and Marinikova air bases also increased following Ukrainian long-range drone attacks on those facilities.

FIGURE 2-5 — RUSSIAN COUNTERSPACE EW SYSTEMS

Russian mobile counterspace EW systems deployed in Eastern Ukraine. Image credit: OSCE [171]

163 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.

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

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

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

167 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; "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/; 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.

168 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/.

169 Dana Goward, "Russia ramps up GPS jamming along with troops at Ukraine border," *GPS World*, April 21, 2021, https://www.gpsworld.com/russia-ramps-up-gps-jamming-along-with-troops-at-ukraine-border/.

170 Sergey Sukhankin, "Blind, Confuse, and Demoralize: Russian Electronic Warfare Operations in Donbas," *Jamestown Foundation*, August 27, 2021, https://jamestown.org/program/blind-confuse-and-demoralize-russian-electronic-warfare-operations-in-donbas/.

171 Ukrainian Mission to OSCE & UN in Vienna (@UKRinOSCE), "Російські новітні системи озброєння - автоматизована станція перешкод Р-330Ж "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-a4b-b86956adc.

In 2023, reports of GPS jamming in Eastern Ukraine intensified. Reports indicated that the GPS jamming was affecting weapons systems that use GPS, such as the Excalibur GPS-guided artillery shells,[172] the High Mobility Artillery Rocket System (HIMARS),[173] and the Joint Direct Attack Munition (JDAM) smart targeting upgrade kit for bombs.[174] It is unknown whether the impacted systems are using the Selective Availability Anti-Spoofing Module (SAASM) anti-jam features introduced in the early 2000s or the newest M-Code encrypted military signals, or whether they are limited to only civil GPS signals.

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 several 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.[175] 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.[176] 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.[177]

In March 2019, the nonprofit C4ADS published an in-depth report on Russian GNSS jamming and spoofing in Russia, Crimea, and Syria.[178] The report details nearly 10,000 suspected incidents across the entire Russian Federation, its occupied territories (including Crimea), and 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, ridesharing 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 air bases in Syria, where weaponized drone attacks have occurred, military EW systems have reportedly been used to spoof GNSS and force attacking drones to land in designated spots.[179] 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 the loss of GPS signals near the airport.[180] The disruptions affected only airborne systems and not terrestrial navigation systems and only occurred during the 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.[181]

In March 2021, the UK Royal Air Force reported GPS jamming affecting its military flight operations out of Cyprus in the Eastern Mediterranean, with suspicion falling on Russian military operations in Syria.[182] In June 2021, the AIS position of a US Navy warship was spoofed to make it appear that it

172 "Russia is starting to make its superiority in electronic warfare count," *The Economist*, November 23, 2023, https://www.economist.com/europe/2023/11/23/russia-is-starting-to-make-its-superiority-in-electronic-warfare-count.

173 Alex Marquardt, Natasha Bertrand, and Zachary Cohen, "Russia's jamming of US-provided rocket systems complicates Ukraine's war effort," CNN, May 6, 2023, https://www.cnn.com/2023/05/05/politics/russia-jamming-himars-rockets-ukraine/index.html.

174 Thomas Whittington, "Jamming JDAM: The threat to US munitions from Russian electronic warfare," *Royal United Services Institute*, June 6, 2023, https://rusi.org/explore-our-research/publications/commentary/jamming-jdam-threat-us-munitions-russian-electronic-warfare.

175 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.

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

177 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.

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

179 "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, https://twitter.com/mod_russia/status/951469288220774401.

180 "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.

181 "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.

182 Thomas Newdick, "Russia is Jamming Royal Air Force Transport Aircraft Flying Out of Cyprus: Reports," *The Drive*, March 19, 2021, https://www.thedrive.com/the-war-zone/39872/russia-is-jamming-royal-air-force-transport-aircraft-flying-out-of-cyprus-reports.

was sailing with a Ukrainian patrol within the territorial waters of Russian-occupied Crimea, when in fact the ship was tied up in port in Odessa.[183]

In March 2022, several aircraft flying near Kaliningrad and also along Finland's eastern border reported interference with their GPS signals. Although the Finnish government did not make any public attributions to the interference, some of it was significant enough to halt flights from Helsinki to Savonlinna in eastern Finland.[184] Additional reports of GPS interference in eastern Finland spike later in 2022 to more than 81 days, four times as many as in early years, and likely a result of the renewed conflict in Ukraine.[185]

The jamming and spoofing of GPS signals in the Eastern Baltic picked up in late 2023 and early 2024, with multiple reports of impacts across broad areas of Finland, Sweden, Poland, Estonia, and Latvia.[186] The spoofing also included the first known cases of "circle spoofing" impacting aviation, where a device's location is altered to make it look like they are circling a fixed point on the ground, usually an international airport. Open source analysis suggests that at least one of the jammers affecting flights in the region is based in Kaliningrad Oblast.[187]

In 2021, new research emerged about a Russian program called Tobol that appears to be aimed at protecting Russian satellites from uplink jamming.[188] 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. Additional sources suggest that there are at least seven Tobol complexes spread across Russian territory, all of which are co-located with satellite tracking facilities.[189] Four are stationary, two are mobile, and the seventh is undetermined as of yet (see Imagery Appendix, pg. 16-28). There is also some evidence to suggest that Russia may be planning a new version or modification to the Tobol system that can attack foreign satellite transmissions, including potentially acting as an uplink jammer for GPS, in addition to (or instead of) protecting Russian satellite transmission.[190] Leaked US military documents suggest that Russia has used at least three Tobol installations to try and disrupt Starlink commercial satellite signals over Eastern Ukraine.[191] Other reports suggest that the GPS jamming and spoofing in the eastern Baltic might be from another Tobol installation in Kaliningrad Oblast.[192]

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.[193]

Russia has also committed to developing 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."[194] The Tirada-2 reportedly can be used to conduct uplink jamming of communications satellites, potentially even capable of causing permanent damage.[195] The Russian Ministry of Defense has publicly stated that the Tirada-2 would enter service in 2019 and three additional versions were in development.[196] Another system reportedly in development is the Bylina-MM, which is designed to "suppress the on-board

183 Thomas Newdick, "U.S. Destroyer Shows Up Right Off Crimea On Vessel Tracking Sites But It Ever Left Port (Updated)," *The Drive*, June 29, 2021, https://www.thedrive.com/the-war-zone/41349/u-s-destroyer-shows-up-right-off-crimea-on-vessel-tracking-sites-but-it-never-left-port.

184 "Finland reports GPS disturbances in aircraft flying over Russia's Kaliningrad," *The Guardian*, Mar 9, 2022, https://www.theguardian.com/world/2022/mar/09/finland-gps-disturbances-aircrafts-russia.

185 Tor Kjetil Kristoffersen, "Russerne jammer Widerøes GPS-er: – Skaper store problemer for oss," Nettavisen, December 22, 2022, https://www.nettavisen.no/nyheter/russerne-jammer-wideroes-gps-er-skaper-store-problemer-for-oss/s/5-95-819901.

186 Dana Goward, "As Baltics see spike in GPS jamming, NATO must respond," *Breaking Defense*, January 31, 2024, https://breakingdefense.com/2024/01/as-baltics-see-spike-in-gps-jamming-nato-must-respond/.

187 DMarkus Jonsson, posting on *Twitter*, January 3, 2024, https://x.com/auonsson/status/1742659031234224220?s=20.

188 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.

189 Bart Hendrickx, posting on the NASASpaceflight.com forums,Bart Hendrickx, "Re: Russian space-related electronic warfare projects," posting to NASA Spaceflight Forums, February 11, 2022, https://forum.nasaspaceflight.com/index.php?topic=52194.msg2340475#msg2340475.

190 Ibid.

191 Alex Horton, "Russia tests secretive weapon to target SpaceX's Starlink in Ukraine," *The Washington Post*, April 18, 2023, https://www.washingtonpost.com/national-security/2023/04/18/discord-leaks-starlink-ukraine/.

192 Ellie Cook, "Secretive' Russian EW system could be behind NATO GPS jamming," *Newsweek*, January 23, 2024, https://www.newsweek.com/russia-electronic-warfare-gps-jamming-nato-finland-poland-sweden-kaliningrad-ukraine-1863096.

193 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.

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

195 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.

196 Ibid.

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.[197]

In September 2018, the Sputnik News service published a report claiming that Russia was developing a new EW aircraft that could be used to target satellite services.[198] The project is aimed at replacing the IL-22PP Porubshchik EW 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.

In March 2022, SpaceX CEO Elon Musk also warned Ukrainian users of his company's Starlink satellite broadband communication system about potential attacks against end user terminals by Russian forces.[199] Musk further claimed that Russia had jammed a Starlink terminal in Ukraine for "hours at a time" before SpaceX was able to ship a software update to mitigate much of the jamming.[200] However, there has not been independent or public validation of the type and magnitude of the jamming and the specific mitigation measures taken.

Additional reports have surfaced of Russian jamming of communications satellites as part of the armed conflict in Eastern Ukraine. One known example was jamming that impacted AMOS-3, a commercial communications satellite providing direct-to-home television broadcasts in Ukraine.[201] Signal analysis suggests the jamming stemmed from a building owned by the Russian Ministry of Defense northeast of Moscow.

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.[202] Due to its range and power, it is also reported to be effective against LEO synthetic aperture radar imaging satellites.[203] 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 EW system against air, space, and ground systems.[204]

In July 2021, several public reports emerged claiming the European Space Agency's Sentinel-1 radar imaging satellite was jammed while imaging locations near the Russian-Ukrainian border.[205] The exact source of the jamming, and whether it was deliberate or not, is uncertain as the Sentinel-1 radar operates in C-Band (around 5 Ghz), which is also used by various ground-based radar systems. Sentinel-1 is used for civil applications, with a relatively low resolution and all of its data publicly accessible, making it unlikely that it was being used for national security purposes. In March 2022, Ukrainian forces captured a containerized command post for the Krashukha-4 system intact near Kyiv.[206]

There is some evidence that Russia is planning a follow-on to its Tobol EW system that might be aimed at preventing optical and radar reconnaissance satellites from imaging Russian territory by blocking the signals they send to data relay satellites.[207]

197 Ibid.

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

199 Jon Brodkin, "Eon Musk: "High" probability of Russian attacks on Starlink in Ukraine," Arstechnica, March 4, 2022, https://arstechnica.com/tech-policy/2022/03/elon-musk-high-probability-of-russian-attacks-on-starlink-in-ukraine/.

200 Valeria Insinna, "SpaceX beating Russian jamming attack was 'eyewatering': DoD official," Breaking Defense, April 20, 2022, https://breakingdefense.com/2022/04/spacex-beating-russian-jamming-attack-was-eyewatering-dod-official/.

201 Michael Clonts, "Tracking interference: The Ukrainian battlefield reaches into space," Kratos Constellations, November 28, 2023, https://www.kratosdefense.com/constellations/articles/tracking-interference-the-ukrainian-battlefield-reaches-into-space.

202 E. Dilipraj, "Electronic Warfare: Russia's Capabilities," *Centre for Air Power Studies*, January 2016, pp.30-32, https://www.researchgate.net/publication/333420461_Electronic_Warfare_Russia's_Enhanced_Capabilities.

203 "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/.

204 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/.

205 Dylan Malyasaov, "Russia is jamming European Space Agency's Sentinel satellite," *Defence Blog*, July 25, 2021, https://defence-blog.com/russia-is-jamming-european-space-agencys-sentinel-satellite/.

206 Joseph Trevithick, "Ukraine Just Captured Part of One of Russia's Most Capable Electronic Warfare Systems," The War Zone, March 22, 2022, https://www.thedrive.com/the-war-zone/44879/ukraine-just-captured-part-of-one-of-russias-most-capable-electronic-warfare-systems.

207 Bart Hendrickx, posting on the NASASpaceflight.com forums, Bart Hendrickx, "Re: Russian space-related electronic warfare projects," posting to NASA Spaceflight Forums, February 15, 2022, https://forum.nasaspaceflight.com/index.php?topic=52194.msg2342023#msg2342023.

208 "Invisible Shield, Invisible Sword: Russia's Electronic Warfare 'Second to None'," *Sputnik News*, August 31, 2017, https://sputniknews.com/20170831/russia-electronic-warfare-system-krasukha-1056962045.html.

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

210 Ibid.

211 Bart Hendrickx, posting on the NASASpaceflight.com forums, Bart Hendrickx, "Re: KB Arsenal's project Ekipazh," posting to the NASA Spaceflight Forum message boards, November 10, 2021, https://forum.nasaspaceflight.com/index.php?topic=48342.msg2309060#msg2309060.

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

FIGURE 2-6 — KRASUKHA-4

A Russian mobile electronic warfare system used to jam radar. Image credit: Sputnik News.[208]

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.[209] 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 EW payloads.[210] KB Arsenal has argued that the nuclear reactor would be powerful enough to support jammers operating on a wide range of frequencies and interfering with electronic systems over a wide area from highly elliptical or geostationary orbits. Additional documentation emerged in 2021 that suggests the purpose of Ekipazh is indeed to develop a nuclear-powered satellite for electronic warfare.[211] 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 the 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.[212] It is much more likely that an EW counterspace weapon would degrade military space capabilities rather than completely deny them.

2.4 — RUSSIAN DIRECTED ENERGY WEAPONS

Assessment /

Russia has a strong technological knowledge base in directed energy physics and is developing a number of military applications for laser systems in a variety of environments. Russia has revived, and continues to evolve, a legacy program whose goal is to develop an aircraft-borne laser system for targeting the optical sensors of imagery reconnaissance satellites, although there is no 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.[213] The most well-known of these was the suspected laser weapons research facility Terra-3 located on the Sary Shagan testing range where the Reagan administration claimed the Soviets were developing advanced anti-satellite laser weapons.[214] There was even a rumor that Terra-3 had been used to lase the Space Shuttle Challenger on October 10, 1984.[215] However, an official US Congressional visit in 1989 found it was more of a "Potemkin village" than an operational weapons site, with lasers that were much less powerful than what the US military already had deployed.[216] 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 the Institute of Atmospheric Optics at Tomsk has developed a laser system with the capability to shoot down drones, using fiber laser technology.[217] 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

212 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/.

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

214 "Soviets could have laser able to blind U.S. satellites," *Gadsden Times*, April 10, 1984, https://news.google.com/newspapers?nid=1891&dat=19840410&id=fqkfAAAAIBAJ&sjid=etYEAAAAIBAJ&pg=2785,2451827.

215 Boris Kononenko,"Silent Space is Being Monitored," *Armeyskiy Sbornik*, June 1996, https://web.archive.org/web/20131224105115/http://www.fas.org/news/russia/1996/drum a189_s96005.htm.

216 Bill Keller, "American Team Gets Closer Look at Soviet Laser," *New York Times*, July 9, 1989, https://www.nytimes.com/1989/07/09/world/american-team-gets-close-look-at-soviet-laser.html.

217 "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.

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.[218]

In 2012, the Ministry of Defense announced the revival of the program.[219] 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.'"[220] The new system, called Sokol-Echelon ("Falcon Echelon"), will be equipped with the 1LK222 laser system, apparently a different system than the original Carbon Dioxide laser type from the 1980s. The new laser reportedly was to be fitted aboard a "brand-new, as-yet-unnamed" aircraft, according to Russian media reports,[221] which turns out to be a modified IL-76MD-90A transport.[222]

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 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 US 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."[223] 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 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 Ajisai. 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. However, recent reports once again suggest that the Russian Ministry of Defense has decided to cancel the program.[224]

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.[225] 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 its troops with laser weapons. Putin called for a public contest to name the system, resulting in "Peresvet," which translates to "over-exposure."[226] 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 (see Imagery Appendix, pg. 16-26).

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

219 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.

220 Patrick Tucker, "Russia Claims It Now Has Lasers to Shoot Satellites," *Defense One*, February 26, 2018, http://www.defenseone.com/technology/2018/02/russia-claims-it-now-has-lasers-shoot-satellites/146243/; "В РФ разрабатывается противоспутниковая система РЭБ," *Ria Novosti*, April 25, 2017, https://topwar.ru/114285-v-rf-razrabatyvaetsya-protivosputnikovaya-sistema-reb.html.

221 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/.

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

223 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.

224 Bart Hendrickx, "Re: Sokol-Eshelon: an airborne laser ASAT system," NASASpaceflight-Forums.com, July 25, 2022, https://forum.nasaspaceflight.com/index.php?topic=50072.msg2389751#msg2389751.

225 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.

226 Ibid.

FIGURE 2-7 — THE PERESVET LASER SYSTEM

A Russian mobile laser system used to dazzle aerial and space reconnaissance assets.
Image credit: Russian Ministry of Defense [227]

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." [228] 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.[229] In May 2022, Russian officials claimed that Peresvet, or potentially an even more advanced version referred to as "Zadira," was being deployed to the conflict in Ukraine.[230] However, there is no evidence to support that claim, and some social media reports of lasers being fired in the sky are likely due to meteorological phenomena rather than laser weapons.[231]

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 (see Imagery Appendix, pg. 16-49). 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. 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.[232] The project appears to be led by the Scientific and Industrial Corporation "Precision Instrument Systems" (NPK SPP). Public documents suggest the contracts were awarded in 2015 and 2018 and satellite imagery suggests that construction work on the project began in August 2019.[233]

227 Ibid.

228 Ibid.

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

230 Amy Chang, "Russian touts new laser weapons, but Ukraine and the U.S. are skeptical," The Washington Post, May 19, 2022, https://www.washingtonpost.com/world/2022/05/19/russia-laser-weapon-zadira-peresvet-ukraine/.

231 Ed Browne, "Fact Check: Did Russia Use Lasers to Target Satellites Over Ukraine Border?" Newsweek, October 5, 2022, https://www.newsweek.com/russia-ukraine-laser-weapon-peresvet-light-1749202.

232 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.

233 Bart Hendrickx, "Kalina: A Russian ground-based laser to dazzle imaging satellites," The Space Review, July 5, 2022, https://www.thespacereview.com/article/4416/1.

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.[234] The idea is similar to historical US proposals such as Project Orion in the 1990s.[235] More recently, NASA Ames proposed a "LightForce" concept for a less powerful laser to deorbit small space debris through radiation pressure.[236] Although NASA ultimately passed on the proposal, it has been picked up by a private company, Electro Optic Systems, and is being developed with support from the Australian government.[237] 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.[238] 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).[239] 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 1970s, the USSR researched the development of a space-based high-power laser for anti-satellite missions.[240] The program resulted in the production of a concept known as Skif-DM (or Polyus). The Skif-DM vehicle was to be a very large spacecraft (approximately 80,000 kg) that was placed in orbit by the very large Energia space launch vehicle used to launch the Buran space shuttle.[241] On May 11, 1987, an attempted launch of an unarmed Skif-DM mock-up was a failure, attributed to an attitude control problem on the payload itself, which re-entered into the Pacific Ocean.[242] The mock-up was reportedly a test vehicle for a one-megawatt carbon dioxide laser.[243] 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.[244]

Operating a high-power space-based laser would be a very demanding technological challenge. Achieving high enough power to damage or destroy satellites would require either a large chemical laser or a large solid-state laser. The chemical laser would require a large store of feed chemicals in order to operate for more than a few seconds. Also, venting of the exhaust gasses 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.

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

235 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.

236 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.

237 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.

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

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

240 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.

241 Ibid.

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

243 Pavel Podvig, "Did Star Wars Help End the Cold War? Soviet Response to the SDI Program," Science and Global Security, 2017, Vol 25 No 1, 3—27, p. 11, https://scienceandglobalsecurity.org/archive/sgs25podvig.pdf.

244 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.

In contrast, the technical and financial challenges to space-based DEW for counterspace remain substantial. These include the 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 potentially large constellation of satellites required. 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.

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 maintains a catalog of Earth-orbiting space objects in LEO that is somewhat smaller than that of 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 (SKKP) consists of multiple phased array radars that are primarily used for missile warning along with dedicated ground-based electro-optical telescopes. Several of the SKKP 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 ABM 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.[245] 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).[246] 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 (see Imagery Appendix, pg. 16-44). 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

245 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.

246 Ibid.

Mukachevo being 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 (see Imagery Appendix, pg. 16-42). 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 kilometers 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.[247] The remaining Dnepr radar sites were planned to be converted over to Voronezh by 2022, with several new sites also being developed.[248] As of 2019, 12 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.

In recent years, Russia has also developed newer radars that are specifically designed for SSA. Razvyazka, also known as 14Ts031, is described as a digital active phased-array antenna operating in the P-band and designed to track space objects as small as 10 cm.[249] The Razvyazka project began in 2009 and is located near the town of Chekhov southwest of Moscow, on the site of a legacy Dunai-3U missile warning radar. In June 2023, the Russian Ministry of Defence reported that the Razvyazka site was finally operational (see Imagery Appendix, pg. 16-47).[250]

Russia's primary optical SSA facility is the Okno ("Window") complex located near the city of Nurek in northern Tajikistan (see Imagery Appendix, pg. 16-51). The Okno facility consists of a cluster of 10 electro-optical telescopes, laid out in 2 clusters of 4 and 6 telescopes each, that are designed to detect space objects at altitudes from 2,000 to 40,000 kilometers, although some reports suggest an additional capability to track space objects down to 120 km and up to 50,000 kilometers, as well as conduct TT&C with Russian civilian satellites.[251] 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.[252] 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.

Russia also operates the Krona radio-optical complex near Storozhevaya in southwestern Russia (see Imagery Appendix, pg. 16-48). Krona uses a combination of radar and optical sensors to track, image, and characterize space objects. The radar, located at 43.826155°N, 41.343355°E, includes both ultra-high frequency (UHF) and super-high frequency (SHF) transmitters. The optical sensor complex (30J6, see Imagery Appendix, pg. 16-49) is located 30 km away at 43.7169171°N, 41.2316883°E and includes a laser locator and electro-optical imager.[253] 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. Another complex, Krona-N, is located at 42°56′8.52″N 132°34′36.37″E, near Nakodka in the Russian Far East.[254]

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.[255] The facility uses a laser rangefinder and a 60-centimeter

247 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.

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

249 Bart Hendrickx, "Re: Russia's space surveillance network," posting on NASASpaceFlight.com forums, June 16, 2023, https://forum.nasaspaceflight.com/index.php?PHPSESSID=g1s1u6hvcf7n3fqklngojfnqei&topic=55993.msg2497800#msg2497800.

250 "Bart Hendrickx, "Re: Russia's space surveillance network," posting on NASASpaceFlight.com forums, June 10, 2022, https://forum.nasaspaceflight.com/index.php?PHPSESSID=g1s1u6hvcf7n3fqklngojfnqei&topic=55993.msg2376324#msg2376324.

251 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.

252 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.

253 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/.

254 Ibid.

255 Allen Thompson, "The Altay Optical-Laser Center Sourcebook," *Federation of American Scientists*, updated March 29, 2011, https://fas.org/spp/military/program/track/altay.pdf.

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 cm or better out to 1,000 km.[256] In 2015, the site was reportedly used to image a US LACROSSE radar reconnaissance satellite.[257] Russia is currently engaged in programs to upgrade many of its SKKP sensors, although its 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,[258] which appears to be a new program called Pritsel ("Target") under the code 14Sh33.[259] The project officially started in 2007 and includes optical telescopes in multiple locations co-located with other types of sensors.

Russia has also announced plans to set up new ground-based observatories in the Nenets Autonomous Region to monitor space objects in polar orbits.[260] 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.[261] 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.[262] 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.[263] 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.[264]

Russia has also been working on a mobile optical sensor complex known as Zorkiy ("sharp-sighted," "vigilant").[265] The project appears to have been proposed as early as 2009 but more recent contracts suggest an actual starting date of 2015. Zorkiy appears to consist of a vehicle-mounted 1.5 m optical telescope along with a second control vehicle and was intended to be used for observing small objects in HEO or GEO orbits from prepared observation sites.

Russian 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 kilometers outside of Moscow.[266] The Centre controls the SKKP 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.[267] ASPOS OKP utilizes data from ISON and other Russian SSA assets to detect and track objects in Earth orbit above 2000 kilometers and provide a range of SSA services, including conjunctions, fragmentations, reentries, and post-mission disposal.

256 Ibid, p. 3.

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

258 "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/.

259 Bart Hendrickx, "Russia's space surveillance network," NASASpaceflight.com forums, March 29, 2022, https://forum.nasaspaceflight.com/index.php?topic=55993.msg2355021#msg2355021

260 Russia to Set Up SSA Observatories Along Arctic Ocean Coast," *SpaceWatchGlobal*, November 2018, https://spacewatch.global/2018/11/russia-to-set-up-ssa-observatories-along-arctic-ocean-coast/.

261 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.

262 Ibid.

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

264 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.

265 Bart Hendricks, "Russia's Space Surveillance Network," NASA Spaceflight forums, March 9, 2022, https://forum.nasaspaceflight.com/index.php?topic=55993.msg2348815#msg2348815.

266 "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.

267 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.

In May 2020, Roscosmos outlined plans for several upgrades to its SSA capabilities under a program called Milky Way.[268] 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 ISS, to complement its existing ground-based telescope network.[269] 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. Another presentation outlined plans to add radiofrequency and radar tracking capabilities to complement optical tracking capabilities.[270]

Evidence suggests that the first of these "Milky Way" complimentary upgrades is complete and is part of the Integrated Observation Complex (OKN) located in Russia's Far East.[271] OKN is a military facility that was primarily designed to monitor telemetry from rocket launches and the upgrades combine optical tracking telescopes with radiofrequency monitoring antennas and a computer control system. Plans announced to have additional OKN sites in Mexico or Cuba appear to be on hold.

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.[272] 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.[273] The Institute for Applied Geophysics contributes to the ISES.

Potential Military Utility /

Russia possesses sophisticated SSA capabilities that allow it to track, identify, and characterize nearly all objects bigger than 10 cm in Earth orbit. While the Russian SKKP possesses many of the same shortcomings of the US 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 adversaries' national security satellites. The ongoing modernization of Russia's SSA capabilities, combined with the modernization of their offensive counterspace capabilities, suggests a focus on developing an integrated operational system for future conflicts that extend into space.

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 US 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

268 "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/.

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

270 Vladimir Agapov, "Неопределённости при оценивании и прогнозировании параметров движения центра масс космических объектов в ОКП, связанные с невозможностью прямого учёта ряда возмущающих факторов негравитационной природы,"2022, http://bsfp.iszf.irk.ru/sites/default/files/school/2022/materials/AgapovVM.pdf.

271 Bart Hendrickx, "Re: Russia's space surveillance network," posting on NASASpaceFlight.com forums, March 31, 2023, https://forum.nasaspaceflight.com/index.php?PHPSESSID=g-1s1u6hvcf7n3fqklngojfnqei&topic=55993.msg2471131#msg2471131.

272 S. Avdyushin et al, "Russian Space Weather Initiatives," *ResearchGate*, January 1999, https://www.researchgate.net/publication/237384438_RUSSIAN_SPACE_WEATHER_INITIATIVES.

273 "Space Weather Today and Possible Effects," *Federal Service for Hydrometeorology and Environmental Monitoring*, accessed February 21, 2020, http://space-weather.ru/index.php?page=home-en.

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 US 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 US 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.[274] 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 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.[275]

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.[276] This concept also appears in the 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 the conflict and, once the 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.[277]

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 US space-based capabilities.

During the late 1990s and early 2000s, 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

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

275 Anton Petrov, "Future Warfare," Moscow Defense Brief, no. 3 (2016), http://www.mdb.cast.ru/mdb/3-2016/item1/article1/.

276 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.

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

ground forces came to partially rely on western-based GPS navigation systems.[278]

Since 2011, Russia has maintained the minimum 24 GLONASS satellites necessary for its military applications.[279] 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 non-contact warfare.[280] 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.[281] In Syria, Russian forces have used satellite-enabled weapons ranging from more accurate air-launched and dropped munitions to sea-based PGM employment.[282] Satellite navigation has also improved Russian situational awareness on the ground.[283]

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.[284] At the operational-strategic level, other systems would challenge western military forces' use of satellite-based communications over large sections of the battlefield.[285] 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.

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 US reliance on space-based capabilities as a potential vulnerability to be exploited during conflict. The Russian forces also see their 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 and Ukraine. However, based on an understanding of the US vulnerability, the Russian military understands that its own space-based capabilities are a vulnerability that must be mitigated through both offensive means and retaining key capabilities and knowledge that is not reliant on space-based information. Finally, the Russian leadership is concerned about the possibility of space-based weapons that can target ground-based assets and critical infrastructure.

One could argue, based on public Russian statements and initiatives, such as promoting treaties against the weaponization of space, that the Russian concern over the militarization of space is in response to US initiatives.[286] 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.[287]

Russian objectives in space, however, face significant challenges over the near term primarily from industry shortcomings.[288] The Ukraine conflict and the subsequent sanctions placed on Russia brought to light several Russian industrial and technological deficiencies in its space program such as the hardening and miniaturization of electronics.[289] Despite these challenges,

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

279 Ibid.

280 Constantine Bogdanov, "Russian Operations in Syria," *Natsional'naia oborona*, no. 12 (2017).

281 Ibid.

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

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

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

285 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.

286 "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.

287 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.

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

289 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.

Russian President Vladimir Putin announced a series of initiatives suggesting that Russia intends to aggressively address its shortfalls in space.[290]

Russia has also made recent statements on its interpretation of attacks against satellites. In March 2022, the head of Roscosmos stated publicly that any cyber attacks on Russian satellites would be taken as a justification for war.[291] In October 2022, a senior Russian official in the Foreign Ministry stated that commercial satellites from the United States and its allies could become legitimate targets if they were involved in the war in Ukraine.[292]

Space and Counterspace Organization

Russian space activities are run by Roscosmos. 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.[293] In its current form, Roscosmos is responsible for Russian 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.[294] 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, maintaining ballistic missile early warning, the satellite control network, and the space surveillance network along with anti-air and anti-missile defense.[295] 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 US capabilities such as the Prompt Global Strike Program.[296]

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.[297] Additionally, Russia maintains five dedicated EW brigades that can provide operational or strategic effects out to several hundred km.[298]

The budget for Russian military space activities was estimated at $1.7 billion in 2020.[299] In 2021, President Putin announced that he planned to cut the budget for Russian space activities across the board by 16 percent annually from 2022 to 2024, citing unhappiness with its performance.[300]

In 2022, more evidence emerged signaling significant budget challenges for the Russian space program. Roscosmos reportedly suffered a huge increase in net losses to $421 million (31 billion rubles) in 2021–2022, and the ongoing war in Ukraine and associated economic sanctions may make that even worse.[301] The budget shortfalls are likely to be exacerbated by Russia's complete severing of its foreign commercial space launch sales as a result of the war in Ukraine.

290 "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.

291 "Russian space agency head says satellite hacking would justify war - report," Reuters, March 2, 2022, https://www.reuters.com/world/russia-space-agency-head-says-satellite-hacking-would-justify-war-report-2022-03-02/.

292 "Russia warns West: We can target your commercial satellites," Reuters, October 27, 2022, https://www.reuters.com/world/russia-says-wests-commercial-satellites-could-be-targets-2022-10-27/.

293 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.

294 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.

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

296 Ibid.

297 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_Electronic_Warfare_to_2025.pdf.

298 Ibid, pp. 7.

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

300 Eric Berger, "Putin slashes Russia's space budget and says he expects better results," *Arstechnica*, October 8, 2021, https://arstechnica.com/science/2021/10/putin-slashes-russias-space-budget-and-says-he-expects-better-results/.

301 Pavel Luzin, "Russian Space Spending for 2023," The Jamestown Foundation, February 10, 2023, https://jamestown.org/program/russian-space-spending-for-2023/.

39.9042°N

03

CHINA

116.4074°E

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 to bolster its national security. China is beginning to assert its regional political, economic, and military interests more strongly, 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 US space capabilities is a key element of China's ability to assure its freedom of action and deter potential US military operations in its sphere of influence.

China has a sustained effort to develop a broad range of offensive 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 offensively use its 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. but operational testing has occurred.

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.

3.1 — 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, 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.[1] The first known incident occurred in LEO in the summer of 2010 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 with 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

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.

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 or 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 US Navy's Multiple Path Beyond Line of Site Communication (MUBLCOM) satellite in April 2005 (see US Co-Orbital ASAT, Section 1.1).[6] As of February 2024, SJ-12 is in a slowly decaying orbit at roughly 550 km.

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 US 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 US military.[11]

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 3-1 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.

3 Ibid.

4 Leiying Xu, "China Sends Research Satellite into Space," *Xinhua*, updatedJ une 15, 2010. http://english.cri.cn/6909/2010/06/15/1821s576844.htm.

5 A more detailed technical analysis of this event can be found in Brian Weeden, "Dancing in the Dark; The Orbital Rendezvous of SJ-12 and SJ06F," *The Space Review*, August 30, 2010, http://www.thespacereview.com/article/1689/1.

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

7 Jonathan McDowell, posting on the NASAspaceflight.com forums, July 20, 2013, http://forum.nasaspaceflight.com/index.php?topic=30486.msg1076481#msg1076481.

8 Posting on the 9ifly.cn Forums, August 8, 2013, http://bbs.9ifly.cn/forum.php?mod=viewthread&tid=9551&page=1#pid261125.

9 Posting on the 9ifly.cn Forums, July 26, 2013, http://bbs.9ifly.cn/forum.php?mod=viewthread&tid=10910&page=16#pid259544.

10 Gunter Krebs, "CX 1," *Gunter's Space Page*, updated November 12, 2017, http://space.skyrocket.de/doc_sdat/cx-1.htm.

11 Due to the uncertainty regarding which payload was which, the public Space Track catalog has not identified which satellite was which. They are still labeled Payload A, Payload B, and Payload C.

FIGURE 3-1 — RPO/ROBOTIC ARM DEMONSTRATOR SY-7

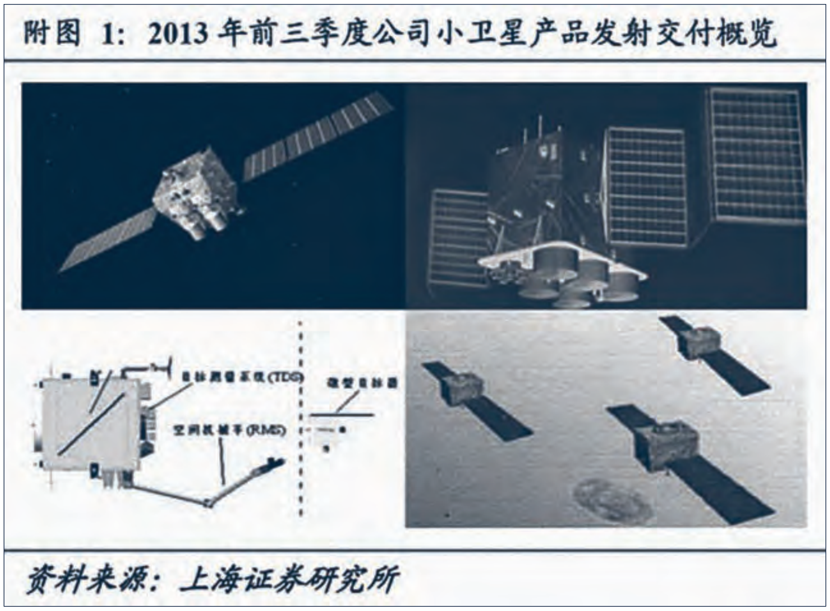


Image of the SY-7 (lower left, with robotic arm) and its small companion satellite. Image credit: Liss [12]

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 US 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 is 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 US 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 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 match orbital planes once again 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] Throughout the rest of May, the SJ-15 slowly decreased the distance to the SJ-7 to within a kilometer.[17]

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

13 Marcia Smith, "Surprise Chinese satellite maneuvers mystify western experts," *Space Policy Online*, updated August 19, 2013, http://spacepolicyonline.com/news/surprise-chinese-satellite-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.

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, bringing it close to the CX-3 again.[18] As of February 2024, SJ-15 is in a slowly decaying orbit at approximately 660 km.

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 the China Academy of Launch Vehicle Technology (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, from Wenchang Space Launch Center (see Imagery Appendix, pg. 16-15) along with a scaled-down test version of China's next human spacecraft, a ballast mass, and a few small rideshare cubesats. The purpose of the launch was to demonstrate the ability of the LM-7 and its restartable upper stage to place the new crewed spacecraft into orbit, to deploy multiple payloads into different orbits, test the new 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 US 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 US military, nor did any of the ten objects cataloged in space rendezvous with any other satellites. According to US 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]

On April 27, 2021, China launched nine small payloads into LEO from Taiyuan Space Launch Center (see Imagery Appendix pg. 16-14) that reportedly carried an orbital debris removal experiment.[25] The NEO-01 payload, developed by Origin Space Technology Company, reportedly carried out an experiment of using a large net to capture a tethered target simulating orbital debris.[26] However, it is difficult to accurately verify if this claim is true as the US military has not identified any of the objects from the launch as a specific payload and it is unclear if any of them released any additional objects. None appeared to have approached any existing pieces of space debris.

18 Posting on NASAspaceflight.com forums, June 7, 2016, http://forum.nasaspaceflight.com/index.php?PHPSESSID=iamdpaq7i-g407ooqdmi8gm06k6&topic=30486.msg1545873#msg1545873.

19 "China lands Prototype Crew Spacecraft after inaugural Long March 7 Launch," *Spaceflight101*, June 27, 2016, http://spaceflight101.com/long-march-7-maiden-launch/china-lands-prototype-crew-spacecraft-after-inaugural-long-march-7-launch/.

20 "Is China militarising space? Experts say new junk collector could be used as anti-satellite weapon," *South China Morning Post*, updated June 12, 2017, http://www.scmp.com/news/china/diplomacy-defence/article/1982526/china-militarising-space-experts-say-new-junk-collector.

21 During a 2011 workshop organized by the National Research Council as part of a study of NASA's space debris program, participants stated that a Department of Defense plan to remove space debris did not go forward in part due to concerns that "most of the proposals had a weapons-like character about them". See National Research Council, *Limiting Future Collision Risk to Spacecraft: An Assessment of NASA's Meteoroid and Orbital Debris Programs*, Washington, DC: National Academies Press, 2011, https://doi.org/10.17226/13244, pg. 143.

22 Jon Fingas, "China successfully refuels a satellite in orbit," *Engadget, July 2*, 2016, https://www.engadget.com/2016/07/02/china-refuels-satellite-in-orbit/.

23 Jeffrey Lin and P.W. Singer, "China's largest space launch vehicle, the Long March 7 flies, with a Technological Triple Whammy," *Popular Science*, July 8, 2016, http://www.popsci.com/chinas-largest-space-launch-vehicle-long-march-7-flies-with-technological-triple-whammy.

24 "Re-Entry: Aolong-1 Space Debris Removal Demonstrator," *Spaceflight101*, August 28, 2016, http://spaceflight101.com/re-entry-aolong-1-space-debris-removal-demonstrator/.

25 Stephen Clark, "Chinese Long March 6 rocket delivers nine small satellites to space," *SpaceflightNow.com*, April 30, 2021, https://spaceflightnow.com/2021/04/30/chinese-long-march-6-rocket-delivers-nine-small-satellites-to-space/.

26 Cao Siqi, "Robot prototype capable of clearing space debris shines at Airshow China," *Global Times*, November 21, 2022, https://www.globaltimes.cn/page/202211/1279404.shtml.

Shenlong Robotic Spaceplane /

In September 2020, China launched an experimental Shenlong 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 (see Imagery Appendix pg. 16-11) under unusually heavy secrecy.[27] Few facts are known, but the US 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 US military cataloged an unknown payload in orbit (Object A, 2020-063G, 46395) while also indicating the spaceplane had re-entered the atmosphere.[28] Outside experts suggested that the spaceplane could have landed on a long runway constructed at China's Lop Nor nuclear test site,[29] ocated in the southeastern portion of the Xinjiang Autonomous Region.[30] The mission of the small satellite it deployed is unknown, although it broadcast transmissions that were similar to a small "companion" satellite released by the Shenzhou 7 crewed spacecraft during a mission in September 2008.[31] Neither the spaceplane nor the subsatellite it released have been registered with the United Nations.

In August 2022, China launched a second Shenlong spaceplane (PRC Test Spacecraft2, 2022-093A, 53357) from Jiuquan Satellite Launch Center (see Imagery Appendix pg. 16-11) into an orbit of 346 km by 593 km at 49.99° inclination. Six pieces of orbital debris from the launch were also cataloged shortly after launch, five of which re-entered the atmosphere by January 2023. On October 23, 2022, the spaceplane raised its perigee significantly to a nearly circular orbit of 607 km by 597 km.[32] Shortly thereafter, a new object (OBJECT J, 2022-093J, 54218), was cataloged that was apparently released from the spaceplane after its orbit-raising maneuver. Neither the spaceplane nor Object J appear to have made any significant maneuvers. Tracking data collected by commercial SSA company LeoLabs suggests that the spaceplane made repeated RPOs with the released object in November 2022, January 2023, and February 2023, including repeated docking, deployment, and formation flying.[33] On May 8, 2023, China state media announced that the second Shenlong spaceplane had re-entered the atmosphere after 276 days in orbit, which again appeared to take place at the Lop Nor facility.[34] As of February 2024, neither object from this second test flight has been registered with the United Nations.

On December 14, 2023, China launched the Shenlong spaceplane (PRC Test Spacecraft 3, 2023-195A, 58573) for the third time, again from Jiuquan Satellite Launch Center (see Imagery Appendix pg. 16-11), into a 333 km by 348 km at 49.99° inclination orbit along with an upper stage and four cataloged pieces of debris.[35] The spaceplane subsequently raised its orbit to 609 km by 601 km in late January 2024, similar to previous missions.[36] There were some reports indicating radio signals emanating from other objects near the spaceplane but were later corrected and as of February 2024, the third Shenlong spaceplane has yet to deploy any additional satellites.[37]

Recent Chinese Rendezvous and Proximity Operations in GEO /

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 from Wenchang Space Launch Complex on Hainan Island (see Imagery Appendix pg. 16-15). 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.[38]

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

28 Data compiled from the public US military satellite catalog at https://space-track.org.

29 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-warzone/36270/this-remote-base-with-a-massive-runway-looks-to-be-where-chinas-secretive-spacecraft-landed.

30 Geoff Brumfiel, "Satellite Photos Show China Expanding Its Mysterious Desert Airfield," *National Public Radio,* July 1, 2021, https://www.npr.org/2021/07/01/1011806020/satellite-photos-show-china-expanding-its-mysterious-desert-airfield?s=09.

31 Andrew Jones, "China's mystery spaceplane releases object into orbit," SpaceNews, November 2, 2022, https://spacenews.com/chinas-mystery-spaceplane-releases-object-in-to-orbit/.

32 Andrew Jones, "China's spaceplane raises orbit and national funding," SpaceNews, October 25, 2022, https://spacenews.com/chinas-space-plane-raises-orbit-and-national-funding/.

33 Joseph Trevithick, "Chinese spaceplane docked with another object multiple times data indicates," *TheWarZone*, May 9, 2023, https://www.twz.com/chinese-spaceplane-docked-with-an-other-object-multiple-times-data-indicates.

34 Andrew Jones, "China's mystery reusable spaceplane lands after 276 days in orbit," *SpaceNews*, May 8, 2023, https://spacenews.com/chinas-mystery-reusable-spaceplane-lands-after-276-days-in-orbit/.

35 Andrew Jones, "China launches mystery reusable spaceplane for the third time," *SpaceNews*, December 14, 2023, https://spacenews.com/china-launches-mystery-reusable-spaceplane-for-third-time/.

36 Andrew Jones, "China's secretive spaceplane raises orbit, but yet to deploy satellites," *SpaceNews*, January 31, 2024, https://spacenews.com/chinas-secretive-spaceplane-raises-its-orbit-but-yet-to-deploy-satellites/.

37 Ibid.

General James Dickinson, then Commander of US Space Command, stated in Congressional testimony that the SJ-17 also carried a robotic arm that could be used for dual use capabilities.[39] The launch was typical of the historical process of getting most satellites to GEO using chemical propulsion,[40] taking about 6 hours and 14 minutes after launch.[41] 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.

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).[42] 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.[43] 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.[44] The two satellites remained close until December 29, when Analytical Graphics, Inc, (AGI) reported that Chinasat 5A had begun drifting away.[45] 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.[46]

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 reverting to zero between July 20-22.[47] 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.[48] 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 1 to determine the source of the anomaly and then monitor the recovery attempt.

Following its rendezvous with Chinasat 1C, the SJ-17 made smaller changes to conduct RPO with Chinasat 6B in January 2020 and SJ-20, a new Chinese high bandwidth communications satellite launched in December 2019, in October 2020. In November 2023, SJ-17 spent a brief period next to VENESAT-1 (2008-055A, 33414), a Venezuelan communications satellite built by China

38 "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/.

39 General James Dickinson, statement before the Senate Armed Services Committee, April 21, 2021, https://www.armed-services.senate.gov/imo/media/doc/Dickinson04.20.2021.pdf.

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

41 "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/.

42 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.

43 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.

44 "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/.

45 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.

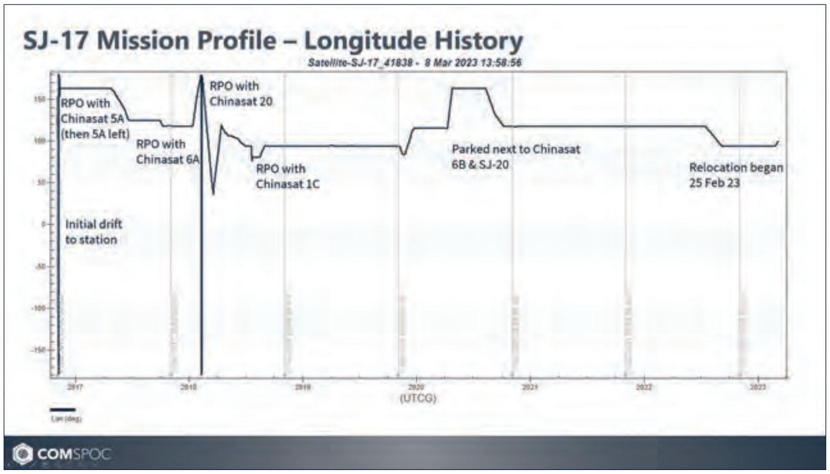
46 Posting by Liss on NASA Spaceflight.com Forum, February 6, 2021, https://forum.nasaspaceflight.com/index.php?topic=39415.msg2189039#msg2189039.

47 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.

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

and launched in 2008. Figure 3-2 summarizes the longitudinal history of the SJ-17 in the geosynchronous region.

FIGURE 3-2 — LONGITUDINAL HISTORY OF THE SJ-17[49]



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.[50] TJS-3 appeared to be similar and the US 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.[51] Object 43917 slowly drifted toward TJS-3 and according to AGI, exhibited photometry consistent with a stabilized object and not one that was tumbling.[52] Thus object 43917 appears to be a subsatellite, not an AKM, and is maintaining a relatively close distance (100 to 200 km) from TJS-3.[53] In May 2019, TJS-3 departed the TJS-AKM and moved to another location, suggesting that it was conducting initial check-out for the first few months while near TJS-AKM. However, its departure was accompanied by an unusual synchronization of maneuvers between TJS-3 and TJS-3 AKM, which some have suggested was a deliberate tactic to complicate tracking of TJS-3.[54]

Since May 2019, TJS-3 has circled the GEO belt and parked relatively close to multiple satellites, including the Russian Luch satellite that has conducted many of its own RPOs in GEO (see Russian Co-Orbital ASAT, Section 2.1), and several US national security satellites (including USA 263, also known as WGS 7, in July 2019, and USA 233, also known as WGS F4, in March 2021 and October 2022) , and has continued to remain active through the end of 2023 as shown in Figure 3-3.[55] However, TJS-3 has typically maintained several hundred km istance from these US military satellites, suggesting it is doing something other than close RPO or has adopted a different pattern of behavior. In December

49 Data compiled by the COMSPOC Corporation.

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

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

52 Ibid.

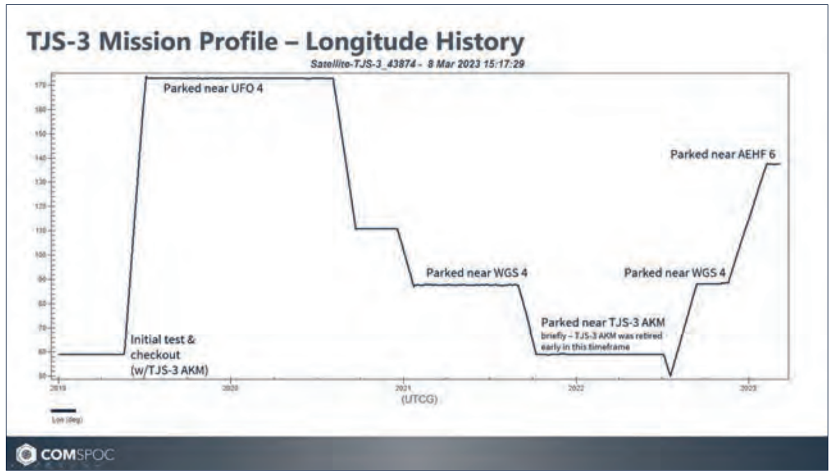
53 Ibid.

54 Colin Clark, "US, China, Russia Test New Space War TacticsL Sats Buzzing, Spoofing, Spying," Breaking Defense, October 28, 2021, https://breakingdefense.com/2021/10/us-china-russia-test-new-space-war-tactics-sats-buzzing-spoofing-spying/.

55 Andrew Jones, "A Chinese spacecraft has been checking out US satellites high above Earth," Space.com, March 3, 2023, https://www.space.com/chinese-spacecraft-tjs-3-inspecting-us-satellites.

2021, TJS-3 AKM raised its orbit significantly above geostationary, which caused it to drift around the entire GEO belt and is now presumed decommissioned.[56]

FIGURE 3-3 — LONGITUDINAL HISTORY OF THE TJS-3[57]



The longitudinal history of the TJS-3 satellite since launch in 2018, including major RPOs with other satellites. Image credit: COMSPOC Corporation.

On October 24, 2021, China launched a classified satellite from the Xichang satellite launch center that it claimed was for a space debris mitigation mission.[58] The satellite, publicly named SJ-21 (49330, 2021-094A) was placed into an initial GTO inclined at 28.5 degrees by a Long March 3B. A statement from the China Aerospace and Technology Corporation, which conducted the launch, stated that it was built by the Shanghai Academy of Spaceflight Technology, and Xinhua reported that the satellite would be used “mainly to test and verify space debris mitigation technologies.”[59] The Shanghai Academy had previously unveiled a “supplemental service spacecraft” designed to refuel satellites on orbit at an airshow two months earlier.[60] By November 2, the SJ-21 used an apogee kick motor to circularize its orbit at about 156E and bring the inclination down to 8°, releasing the AKM as a piece of debris afterward. SJ-21 began drifting slowly westward at about 1 degree per day, although still inclined to geostationary orbit. For a while, SJ-21 maintained close proximity to the AKM, which suggested it was conducting an RPO.[61]

On December 25, 2021, the SJ-21 rendezvoused with a defunct Chinese navigation satellite, Compass G2 (34779, 2009-018A). The Compass G2 was a second-generation navigation satellite launched in 2009 as part of China’s Beidou constellation and appeared to fail early in its orbital lifetime as it lost station keeping and began to drift both east-west and increase in inclination. Compass G2 also experienced a fragmentation event in 2016 that released at least six trackable pieces of debris.[62] While maintaining tight proximity to Compass G2 for several weeks, the SJ-21 docked to it at some point and then around January 21, 2022, used its onboard propulsion to pull both satellites to a higher altitude above the geostationary belt. By January 27, 2022, both objects were in an elliptical orbit ranging from 290 km to 3,100 km above the protected GEO zone, as observed by commercial trackers.[63] Shortly thereafter, SJ-21 reduced its orbital altitude back down to close to GEO, although maintained an inclination slightly higher than 8°. As of February 2023, the SJ-21 has not been registered with the United Nations.

On December 23, 2021, China launched a pair of satellites into GEO orbit as part of the Shiyan series officially labeled Shiyan-12 01 (2021-129A, 50321)

56 T.S. Kelso, Tweet, January 25, 2022, “The object identified as TJS-3 AKM has completed a circuit of the GEO belt, 2 months after it maneuvered well above the threshold for the GEO graveyard. It is presumed to have been decommissioned and its ops status in the CelesTrak SATCAT is being changed to reflect that,” https://twitter.com/TSKelso/status/1486138895196512256?s=20&t=CYW-fr_ZABBtnxffeSn-y2Q.

57 Data compiled by the COMSPOC Corporation.

58 Stephen Clark, “China says its launched a space debris mitigation tech demo satellite,” Spaceflight Now, October 25, 2021, https://spaceflightnow.com/2021/10/25/china-says-it-has-launched-a-space-debris-mitigation-tech-demo-satellite/.

59 Ibid.

60 Andrew Jones, “China launches classified space debris mitigation technology satellite,” *SpaceNews*, October 24, 2021, https://spacenews.com/china-launches-classified-space-debris-mitigation-technology-satellite/.

61 Andrew Jones, “An object is now alongside China’s Shijian-21 debris mitigation satellite,” *SpaceNews*, November 5, 2021, https://spacenews.com/an-object-is-now-orbiting-alongside-chinas-shijian-21-debris-mitigation-satellite/.

62 “Orbital Debris Quarterly News,” NASA Orbital Debris Program Office, Volume 20, Issue 4, October 2016, https://orbitaldebris.jsc.nasa.gov/quarterly-news/pdfs/odqnv20i4.pdf.

63 Theresa Hitchens, “China’s SJ-21 ‘tugs’ dead satellite out of GEO belt: Trackers,” *Breaking-Defense*, January 26, 2022, https://breakingdefense.com/2022/01/chinas-sj-21-tugs-dead-satellite-out-of-geo-belt-trackers/.

64 Andrew Jones, “Long March 7A launches classified Shiyan-12 satellites,” *SpaceNews*, December 23, 2021, https://spacenews.com/long-march-7a-launches-classified-shiyan-12-satellites/.

and Syhiyan-12 02 (2021-129B, 50322).[64] The two satellites remained relatively close to each other in GEO, indicating that they had maneuvering capability and may have been conducting RPO. In late January 2023, USA 270, one of the four American GSSAP intelligence collection satellites (see US Co-Orbital ASAT, Section 1.1) maneuvered to approach SY-12 (01) and SY-12 (02). According to tracking data collected by ExoAnalytic Solutions, SY-12 01 and SY-12 02 made significant maneuvers to split up and begin rotating around the GEO belt in opposite directions, with SY-12 02 apparently also getting an imaging opportunity on USA 270.[65] A video animation released by COMSPOC Corporation also shows the encounter.[66]

On January 8, 2023, China launched a satellite identified as SJ-23 (2023-002A, 55131) into a GTO using a Long March 7A from the Wenchang spaceport on Hainan island. China state media described the satellite as being used for "scientific experiments and technical verification" but provided no further details.[67] Around January 15, the SJ-23 appeared to release another object, which was cataloged as an apogee kick motor (2023-002C, 55180) but may be a functioning satellite.[68] Analysis of the orbital data suggests that the two objects were within 10 km as of late February. The activities of all the aforementioned Chinese RPO satellites are consistent with the demonstration of RPO technologies for 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.[69]

That said, there is evidence to suggest there is more than one category of RPO missions being performed. For example, the SJ-17 has maintained long periods of time relatively close to other communications satellites, while the SY-12 01 and 02 pair have largely been drifting through the GEO belt. This suggests they are being used for a different purpose.

TABLE 3-1 — RECENT CHINESE RPOs

DATE(S)	SYSTEM(S)	ORBITAL PARAMETERS	NOTES
June – Aug. 2010	SJ-O6F, SJ-12	570-600 km; 97.6°	SJ-12 maneuvered to rendezvous with SJ-06F. Satellites may have bumped into each other.
July 2013 – May 2016	SY-7, CX-3, SJ-15	Approx. 670 km; 98°	SY-7 released an additional object that 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 AKM	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. Both satellites then maneuvered away from each other.
May 2019 – Feb. 2023	TJS-3, Luch, USA 233, USA 263, Chinasat 10, Chinasat 16, SJ-20, Chinasat 12	35,600 km; 0°	TJS-3 drifted around the GEO belt, periodically stopping to conduct RPO with other satellites.

65 Debra Werner, "An In-Orbit Game of Cat and Mouse: CLose approaches prompt calls for communications and norms," *SpaceNews*, June 16, 2022, https://spacenews.com/an-in-orbit-game-of-cat-and-mouse-close-approaches-prompt-calls-for-communications-and-norms/.

66 SpaceNewsInc,"USA 270/Shiyan12 encounter," Youtube, Accessed February 22, 2023, https://www.youtube.com/watch?v=H0ZlgmdjXjw.

69 Andrew Jones, "Pair of Chinese launches put classified and commercial satellites in orbit," *SpaceNews*, January 9, 2023, https://spacenews.com/pair-of-chinese-launches-put-classified-and-commercial-satellites-into-orbit/.

69 Andrew Jones, "Classified Chinese satellite releases small object in orbit," *Space.com*, January 24, 2023, https://www.space.com/classified-chinese-satellite-shijian-23-releases-subsatellite.

69 Defense Intelligence Agency, "Challenges to Security in Space," February 2019, https://apps.dtic.mil/sti/pdfs/AD1082341.pdf.

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

70 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.

71 Stephen Chen, "Chinese scientists build anti-satellite weapons that can cause explosion inside exhaust," South China Morning Post, October 21, 2021, https://www.scmp.com/news/china/military/article/3153174/chinese-scientists-build-anti-satellite-weapon-can-cause.

DATE(S)	SYSTEM(S)	ORBITAL PARAMETERS	NOTES
Jan.– Aug. 2020	Chinasat 6B, SJ-20, SJ-17	35,600 km; 0°	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.
Nov. 2022	VENESAT-1, SJ-17	35,600 km; 0°	SJ-17 made a brief RPO with VENESAT-1, a Venezuelan communications satellite built and launched by China in 2008.
Dec. 2021 – Jan. 2022	SJ-21, Compass G2	35,876 km; 8°	SJ-21 maneuvered to dock with Compass G2 and pull it into a much higher orbit.
Nov. 2022 - Feb. 2023	PRC Test Spacecraft 2, Object J	–	PRC Test Spacecraft 2 (Shenlong spaceplane) released Object J and made multiple RPOs, including repeated docking, deployment, and formation flying.

Potential Military Utility /

The most likely military utility of the capabilities demonstrated by the SJ-12, SJ-15, SJ-17, TJS-3 AKM, TJS-3, SJ-21, and SJ-12 (01) and (02) satellites is for on-orbit space situational awareness (SSA) and satellite servicing. Their operational pattern was consistent with slow, methodical, and careful approaches to rendezvous with other space objects in similar orbits. The satellites the SJ-12 and SJ-15 approached were in relatively similar orbits, differing in altitude by a couple of hundred kilometers and slightly in inclination. They did not make huge changes to rendezvous with satellites in significantly different orbits. This behavior is similar to several US RPO missions to test and demonstrate satellite inspection and servicing capabilities such as the XSS-11, which conducted inspections of satellites in LEO in 2005 and 2006 and DARPA's OrbitalExpress satellite that did satellite servicing demonstrations 2007 (see US Co-Orbital ASAT, Section 1.1).

The SJ-17's approach to Chinasat 5A was not inconsistent with the way other active satellites in the GEO belt relocate to different orbital slots. It is also not unusual for satellites to be co-located within several tens of kilometers to share a GEO slot, although it is rare for them to approach within 1 km as the SJ-17 eventually did. Such a close approach in GEO could be used for very detailed imaging or inspection of another satellite or to intercept radio frequency signals directed at another satellite from Earth. Likely examples of the latter are the activities of the US PAN satellite (35815, 2009-047A) between 2009 and 2014 (see US Co-Orbital ASAT, Section 1.1), and the Russian Luch/Olymp satellite (40258, 2014-058A) beginning in 2015 (see Russian Co-Orbital ASAT, Section 2.1).

While the known on-orbit activities of the SJ-12, SJ-15, SJ-17, TJS-3 AKM, and SJ-21 did not include explicit testing of offensive capabilities or aggressive maneuvers, it is possible that the technologies they tested could be used for offensive purposes in the future. One potential offensive use would be to get a radio-frequency jammer close to a satellite, thereby greatly amplifying its ability to interfere with the satellite's communications. While possible, to date there is no direct public evidence of such systems being tested on orbit, although there have been multiple research articles published in Chinese journals discussing and evaluating the concept.[70] A more recent paper from Chinese researchers suggests that they are studying the ability to use RPO capabilities to plant small explosive charges in the nozzle of a spacecraft's engine, although only ground tests are reported so far.[71]

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 involve 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. The 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 — 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 (medium Earth orbit, or 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 the 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.[72]

These various subsidiaries have, over time, been consolidated into large state-owned companies, yet have retained deep-seated direct ties to the military—particularly regarding the 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.[73]

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

72 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.

73 Ibid.

within Program 863.[74] 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.[75] The HQ-19 is a solid-propelled high altitude hit-to-kill (HTK) intercept system roughly equivalent to the US 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 3-2. The first known tests were in 2005 and 2006, both from Xichang Satellite Launch Center in Sichuan (see Imagery Appendix, pg. 16-16), and appear to have been tests of the missile itself.[76] 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.[77] The system was reportedly tested again in 2010 and 2013 from the Korla Missile Test Complex (see Imagery Appendix, pg. 16-13) with successful intercepts of a ballistic target. The move from Xichang to Korla may indicate the system entered a new phase of development, or possibly even operational testing. In April 2021, the US Office of the Director of National Intelligence assessed that China had "fielded ground-based ASAT missiles intended to destroy satellites in LEO."[78]

Naming Convention for Chinese DA-ASATs

The naming conventions for Chinese DA-ASATs are complicated and uncertain. The US 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 US 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 translating to "Kinetic Energy." Although this is somewhat in line with the taxonomy for China's 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 US news reports citing anonymous US officials. Thus, the DN-X designation may be a leak of the Chinese internal name for the system as divined by US intelligence. If so, that suggests that DN-1 is the Chinese designation for the SC-19, DN-2 is the longer range GEO version, and DN-3 could be an upgraded LEO version or a midcourse missile defense interceptor.

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.[79] 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.[80]

74 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.

75 Mark Stokes and Dean Cheng, 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.

76 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.

77 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.

78 "Annual Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence, April 9, 2021, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

79 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)", MissileThreat, 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.

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

FIGURE 3-4 — DF-21 MRBM

Missile version upon which the SC-19 is likely based, mounted atop a TEL. Image credit: Defence Blog.[81]

The organizational history of the SC-19 yields further clues. Chinese rocket development is centralized in two state-owned corporations. According to Chinese bloggers, CASIC sought to leverage the DF-21 and its expertise in solid rockets to develop a new line of solid rocket space launch vehicles (SLV).[82] 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.[83] A US 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,"[84] but unofficial US government sources say it was a test of a new ballistic missile related to China's ASAT program.[85] 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 warning of the flight path in case of complications covered a ground track lining up with a GEO launch trajectory,[86] 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 is no evidence that it "released a barium cloud" as claimed by CAS, nor has there been any subsequent scientific research published because of the launch.

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

82 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.

83 "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.

84 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.

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

86 "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.

Analysis of the launch site also points to something other than either an orbital or sounding rocket.[87] 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 [88], whereas the US military claimed it went "nearly to GEO" at 36,000 km. US officials also stated that the upper stages re-entered the Earth's atmosphere "over the Indian Ocean".[89] A technical analysis concluded that re-entry location is only possible if the apogee was at least 30,000 km; if the apogee was only 10,000 km, the Earth would not have had enough time to rotate for it to land in the Indian Ocean.[90] 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), commonly associated with mobile ballistic missiles, located on a purpose-built launch pad towards the southeast corner of Xichang (see Imagery Appendix, pg. 16-17), as shown in Figure 3-5.[91] 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 US-China Economic and Security Review Commission labeled this new rocket as DN-2 and claimed it may reach operational status in 2020-2025.[92] However, the only known sources of this designation are news reports that cite anonymous US defense officials.[93]

FIGURE 3-5 — XICHANG SPACE LAUNCH COMPLEX ON APRIL 3, 2013

Imagery shows a TEL on the southeast pad. Image © 2013 DigitalGlobe. All rights reserved.
For media licensing options, please contact info@swfound.org

In 2014, China conducted another rocket test, this time claiming that it was part of a missile defense interceptor program.[94] Very little information is

87 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.

88 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.

89 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.

90 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.

91 Ibid.

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

93 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/.

94 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/.

available in the public record about this launch, other than that it occurred, remained suborbital, and does not appear to have had an 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."[95] 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.[96]

Since 2014, evidence suggests China has conducted at least six 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.[97] Photos from another test on July 22, this time launched from Jiuquan Satellite Launch Center (see Imagery Appendix, pg. 16-11) were captured by a pilot on a Dutch commercial airliner flying over the Himalayas.[98] On February 5, 2018, Chinese state media announced it had carried out "land-based midcourse missile interception test within its territory."[99] In all three cases, anonymous US officials were cited by news sources claiming that the tests were of a system known publicly as DN-3 and labeled by US intelligence agencies as KO-09 (as the ninth missile type seen out of Korla).[100] DN-3 could refer to an upgraded version of the LEO-capable DN-1 or an adaptation of the same weapon system for midcourse missile defense, akin to the US sea-based Standard Missile (SM)-3 interceptor or Ground-based Interceptor (GBI), with latent ASAT capabilities (see US DA-ASAT, Section 1.2).[101] China publicly announced additional "land-based midcourse missile intercept technology test[s]" on February 4, 2021,[102] and June 21, 2022,[103] and April 14, 2023,[104] with very similar descriptions as previous tests of the DN-1 and its derivatives.

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."[105] 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."[106] 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.

TABLE 3-2 — HISTORY OF CHINESE DA-ASAT TESTS[107]

DATE	SYSTEM	LAUNCH SITE	PAYLOAD	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, debris created
Jan. 11, 2010	SC-19	Korla	CSS-X-11 ballistic missile launched from Jiuquan	250 km	Destruction of suborbital target

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

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

97 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.

98 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/.

99 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/.

100 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/.

101 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/.

102 Wang Xinjuan, "China conducts land-based mid-course missile interception test," Chinese Ministry of National Defense, February 5, 2021, http://eng.chinamil.com.cn/view/2021-02/05/content_9980841.htm.

103 Emma Helfrich, "China Conducts Midcourse Missile Defense Test One Year After Last," The Warzone, June 21, 2022, https://www.thedrive.com/the-war-zone/china-conducts-sixth-missile-defense-test-one-year-after-the-last-one.

104 "China says it conducted mid-course missile interception test," *Associated Press*, April 15, 2023, https://apnews.com/article/china-interceptor-missile-test-defense-c77ae53a43f5e74bc48c4be45e46af80.

105 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.

106 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.

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

DATE	SYSTEM	LAUNCH SITE	PAYLOAD	APOGEE	NOTES
Jan. 27, 2013	Possible SC-19	Korla	Unknown ballistic missile launched from Jiuquan	Suborbital	Destruction of suborbital target
May 13, 2013	Possible DN-2	Xichang	None known	~30,000 km	Likely rocket test
July 23, 2014	Possible DN-2	Korla? (Jiuquan?)	Likely ballistic missile launched from Jiuquan	Suborbital	Likely intercept test
Oct. 30, 2015	Possible DN-3	Korla	None known, possible ballistic missile	Suborbital	Likely rocket test
July 23, 2017	Possible DN-3	Jiuquan?	Likely ballistic missile	Suborbital, malfunctioned	Likely intercept test
Feb. 5, 2018	Possible DN-3	Korla	Likely ballistic missile	Suborbital	Likely intercept test
Feb. 4, 2021	Possible DN-3	Korla	Likely ballistic missile	Suborbital	Likely intercept test
Jun. 19, 2022	Possible DN-3	Korla	Likely ballistic missile	Suborbital	Likely intercept test
Apr. 14, 2023	Possible DN-3	Korla	Likely ballistic missile	Suborbital	Likely intercept test

There has been speculation by Western analysts that China may also have sea- or air-based capabilities that could be used as DA-ASATs. Some have suggested that the JL-2 submarine-launched ballistic missile (SLBM) developed for basing on China's JIN-class SSBNs may have an ASAT capability. Others have suggested China may be developing an air-launched DA-ASAT, similar to the US ASM-135 (see US Direct-Ascent ASAT, Section 1.2) 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.

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

At the same time, there are also constraints on the military utility of such systems, particularly as China improves its space capabilities. The use of a kinetic 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 military satellites and space capabilities, the long-lasting debris from the use of DA-ASATs will be increasingly likely to threaten their own capabilities. The 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.

3.3 — CHINESE ELECTRONIC WARFARE

Assessment /

China is likely to have significant EW counterspace capabilities against 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 /

GNSS Jamming

GNSS jamming, particularly of the US 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.[108] 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.[109] 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

108 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.

109 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/.

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 stated 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.[110]

SAR Jamming

The January 2019 US DIA space and counterspace report stated 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.[111]

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.[112] 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.

Space-Based Jamming

In November 2023, new research emerged indicating that Chinese military authors had been discussing the apparent prevalence of space-based jamming of satellite capabilities by other space powers, notably the United States and Russia.[113] No public evidence exists of such jamming being done by any country, but several states included a mention of space-based jamming as a growing threat in their submissions and statements to the U.N. General Assembly Resolution 75/36 in 2021.[114]

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,

110 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.

111 Ibid.

112 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.

113 Kristin Burke, “Is military space-based jamming normal? Some worry it is,” War on the Rocks, November 13, 2023, https://warontherocks.com/2023/11/is-military-space-based-jamming-normal-some-worry-it-is/.

114 Ibid.

and procedures exist to mitigate attacks.[115] It is much more likely that an EW counterspace weapon would degrade military space capabilities rather than completely deny them.

3.4 — 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 /
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.[116] However, information about how advanced Chinese DEW counterspace weapons are remains unknown and there is very little public evidence of their deployment or use.

Open-source research suggests at least five main sites are supporting China's DEW work.[117] 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 (see Imagery Appendix, pg. 16-29). Both facilities have strikingly similar large, rectangular buildings with retractable roofs and suggest facilities where DEW aimed at satellites could have been developed. A third site is located near the Korla Missile Test facility in Xinjiang Province, known as "Korla", "Bosten Lake", or "Bohu",[118] and features camouflaged buildings and security fences that strongly suggest it is military-operated (see Imagery Appendix, pg. 16-30). 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.[119] Evidence suggests that Unit 63655 of the Strategic Support Force operates the Korla/Bohu complex.[120] In May 2023, the US commercial satellite remote sensing company BlackSky reported seeing the roof of the Korla East facility open during multiple satellite passes and large lasers inside that looked like larger versions of the Silent Hunter vehicle-mounted tactical laser system.[121]

In 2006, a report by Defense News cited anonymous US defense officials who claimed that China had used ground-based lasers to "dazzle" or blind US optical surveillance satellites on multiple occasions.[122] Subsequent reporting suggested that the satellites may have been merely illuminated by the lasers and senior US officials at the time stated that no US satellites were materially damaged. A Chinese scientific journal also documented a successful test in 2005 of a vehicle mounted laser stationed in Xinjiang.[123]

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.[124]

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, although did not provide more specifics.[125] The January 2019 DIA space and counterspace report stated that China is likely pursuing laser weapons for counterspace applications

115 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/.

116 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.

117 Based on personal communication with Sean O'Conner.

118 Eli Hayes, "The Bohu Laser Facility, Part 1: History and Organization," Arms Control Wonk blog, December 20, 2022, https://www.armscontrolwonk.com/archive/1216848/the-bohu-laser-facility-part-1-history-and-organisation/.

119 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/.

120 Eli Hayes, "The Bohu Laser Facility, Part 1: History and Organization," Arms Control Wonk blog, December 20, 2022, https://www.armscontrolwonk.com/archive/1216848/the-bohu-laser-facility-part-1-history-and-organisation/.

121 Andrew Salerno-Garthwaite, "Is China's Korla laser ASAT site hacking Western satellites," Army Technology, May 1, 2023, https://www.army-technology.com/features/is-chinas-korla-laser-asat-site-hacking-western-satellites/?cf-view=.

122 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.

123 Minghui Gao, Yuquan Zheng, and Zhihong Wang, 'Development of Space-Based Laser Weapons', Chinese Optics 20:6 (2013): 810–17.

124 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.

125 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.

and assessed that China will likely field a ground-based laser weapon by 2020, although this has not yet been confirmed.[126] 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. Additional open source research suggests that the Korla/Bohu complex is the main site for this R&D and it may be aimed at developing vehicle-mounted dazzling or destructive lasers.[127]

In December 2021, a Chinese research team from Zhejiang University published a paper documenting their development of a "small but powerful" laser that could be used for several different applications in space.[128] The research team created a laser that weighs 1.5 kilograms and can deliver 5 nanosecond pulses of about 5 millijoules each at up to 100 times per second for 30 minutes before overheating. While it is not powerful enough to do physical damage to another space object, the research suggests significant improvements in power to weight ratio for space-capable laser systems.

In March 2022, a team of Chinese scientists reported development of a high-powered relativistic klystron amplifier (RKA) that could create short pulses of up to 5 megawatts in the Ka frequency band.[129] RKAs are a decades-old technology for creating high-power microwave beams and have broad applications in radars, particle accelerators, and communications systems. While not a new technology, RKA development has posed challenges in both increasing the power of the beams and moving to high frequencies. One application of this new development by Chinese scientists could be satellite-mounted RKAs that could be used to damage or interfere with the electronics of other satellites from relatively close range. Around the same time, a different group of Chinese scientists published their own research on new ways to protect satellites against attacks by high-power microwave weapons.[130]

In March 2023, another group of Chinese military scientists reported that they had developed a small pulse power device that could generate a 10-gigawatt electron beam, which in turn could be small and powerful enough to drive a high-power microwave beam weapon.[131] Another report in February 2024 indicated that researchers had successfully used a Stirling engine to power a high-power microwave beam weapon, which could greatly increase its efficiency and ability to operate for longer periods of time.[132]

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 the 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 a 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

126 Defense Intelligence Agency, "Challenges to Security in Space," January 2019, p. 20, https://apps.dtic.mil/sti/pdfs/AD1082341.pdf.

127 Eli Lake, "The Bohu Laser Facility, Part 2: Operations," Arms Control Wonk blog, December 21, 2022, https://www.armscontrolwonk.com/archive/1216867/the-bohu-laser-facility-part-2-operations/.

128 Stephen Chen, "The powerful Chinese megawatt laser 'small enough for a satellite'," *South China Morning Post*, January 7, 2022, https://www.scmp.com/news/china/science/article/3162566/chinese-megawatt-laser-powerful-small-enough-be-used-satellite.

129 Gabriel Honrada, "China in a microwave weapon great leap forward," Asia Times, March 17, 2022, https://asiatimes.com/2022/03/china-in-a-microwave-weapon-great-leap-forward/.

130 Stephen Chen, "New device could protect satellites from microwave attacks, say Chinese scientists," South China Morning Post, February 23, 2022, https://www.scmp.com/news/china/science/article/3167937/chinese-scientists-say-new-device-could-protect-satellites.

131 Stephen Chen, "Scientists shrink China's Starlink-killing microwave weapon with a new power source," *South China Morning Post*, March 30, 2023, https://www.scmp.com/news/china/science/article/3214251/scientists-shrink-chinas-starlink-killing-microwave-weapon-new-power-source.

132 Stephen Chen, "Chinese scientists build powerful microwave weapon that can fire from a moving truck, using Stirling engine to cool technology," *South China Morning Post*, February 8, 2024, https://www.scmp.com/news/china/science/article/3251381/chinese-scientists-build-powerful-stirling-engine-based-microwave-weapon-can-fire-moving-truck.

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 — 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 aids in its ability to characterize and collect intelligence on foreign satellites.

Specifics /
China's main optical SSA capabilities are operated by the Purple Mountain Observatory (PMO) (see Imagery Appendix, pg. 16-52), which operates multiple telescopes in seven separate locations that can track satellites throughout all orbital regimes.[133] 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 researches orbital debris.[134]

Few details are known about China's radar SSA capabilities as they are primarily operated by the PLA. The PLA operates at least six large phased-array radars (LPARs) (see Imagery Appendix, pg. 16-50) that likely have a primary mission of ballistic missile warning but could also support an SSA mission. The existing radars are located near Huanan (46.53N, 130.76E), Hangzhou (30.29N, 119.13E), Korla (41.64N, 86.24E), Kongtong (35.4829 N 106.571 E), and two radars at Yiyuan (36.02N, 118.09E).[135] The radars are approximately 30 meters in diameter and likely have a coverage arc of 90 to 120 degrees, similar to a US BMEWS radar (see US Space Situational Awareness Capabilities, Section 1.5).[136] The Korla radar can be rotated and is likely used to support the ballistic missile and ASAT testing done at Korla.

In June 2021, China held a ceremony to break ground on a new tracking telescope in Xining, Qinghai Province. The announced plans include the construction of a large array of telescopes called the Multi-Application Survey Telescope Array (MASTA) that will mainly be used to detect space objects above LEO.[137] The project is being managed by the Purple Mountain Observatory and is expected to be completed in 2023.

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.[138] Officials stated that the Center would provide early warnings of close approaches and possible collisions to Chinese satellite operators. In January 2022, the Space Debris Monitoring and Applications Center sent a warning about a close approach between a piece of debris from the November 2021 Russian ASAT test and a Chinese science satellite. The analysis provided by

133 "About Purple Mountain Observatory (PMO)," *Purple Mountain Observatory*, accessed February 28, 2022, http://english.pmo.cas.cn/au/.

134 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.

135 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; James Acton, "ADDENDUM. Turns out China actually has a SIXTH publicly documented ballistic missile EW radar. There's two at Yiyuan (shame on me for missing this). H/T @luritie This faces NE and provides coverage of the Pacific. (20/20)," posting on X, March 30, 2023, https://x.com/james_acton32/status/1641428299682291712?s=20.

136 Ibid.

137 "New survey telescope in NW China's Qinghai will help detect space debris in medium and high orbits," *Global Times*, June 28, 2021, https://www.globaltimes.cn/page/202106/1227223.shtml.

138 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.

the Center suggested that a piece of Cosmos 1408 debris would pass within 14.5 meters of the Tsinghua Science satellite, a small satellite launched in 2020 to provide Earth observation.[139]

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.[140] 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.[141] 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.[142] However, to date, there is no evidence that the international TT&C sites operated by China are fundamentally different from similar sites 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 organization for space cooperation that includes Bangladesh, Iran, Mongolia, Pakistan, Peru, Thailand, and Turkey as members and Mexico as an observer.[143] 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.[144] 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).[145] While some publications have described APOSOS as being fully capable of providing global GEO coverage,[146] publications from ASPCO suggest the project is still nascent and has only limited capabilities.

In June 2023, Egypt announced it was building a new satellite tracking station in cooperation with China.[147] The facility will include two optical telescopes with diameters of 120 cm and 70 cm, as well as lasers for rangefinding.

China's work on space weather is conducted through the National Space Weather Monitoring and Warning Center, which was established by the Central Planning Committee in 2002 and is part of the China Meteorological Administration.[148] The Center provides daily space weather forecasts and warnings of severe space weather based mainly from 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.[149]

Potential 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

139 Fan Wei, "Following 'extremely dangerous rendezvous' between Russian space debris and Chinese satellite, Chinese expert says it's possible the two get closer again," *Global Times*, January 20, 2022, https://www.globaltimes.cn/page/202201/1246440.shtml.

140 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.

141 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/.

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

143 "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.

144 "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.

145 NewsAPSCO," *Asia-Pacific Space Cooperation Organization*, April 2019, http://www.apsco.int/upload/file/20190508/2019050809583923213.pdf.

146 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.

147 "Egypt to establish 2nd largest monitoring station for satellites, space debris globally," *Egypt Independent*, June 8, 2023, https://egyptindependent.com/egypt-to-establish-2nd-largest-monitoring-station-for-satellites-space-debris-globally/.

148 "Space Weather Products," National Center for Space Weather, accessed February 18, 2020, http://www.nsmc.org.cn/NSMC/spaceweather/en/sws/index.html.

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

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 the 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.

3.6 — 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, unofficially 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 reorganized its space and counterspace forces, as part of a larger military reorganization, and placed them in a new major force structure that also has control over electronic warfare and cyber. China's considerable investment in developing and testing counterspace capabilities, as detailed in this chapter, suggest they see space as a domain for future conflicts, whether or not that is officially stated. 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 US aggression. There is no public evidence of China actively using destructive counterspace capabilities in current military operations, although it is likely they are using SSA and electronic warfare in at least some support roles.

Specifics /

Chinese Views on Space Warfare

Official Chinese public statements on space warfare and space weapons have remained consistent: "China always adheres to the principle of the use of outer space for peaceful purposes and opposes the weaponization of or an arms race in outer space" and Chinese officials have made an explicit distinction between their views and the recent US public declaration of space as a warfighting domain (see US Counterspace Policy, Doctrine, and Organization, Section 1.6).[150] However, since 2015, other official writings suggest China's internal 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." [151] 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.[152] China's

150 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; "China firmly opposes arms race in outer space: defense spokesperson," Xinhua, December 14, 2023, https://english.news.cn/20231214/c0eec39b9f634023b91daaac8f1aa751/c.html.

151 *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/.

152 "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.

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

2010 defense white paper, "China's National Defense in the New Era", stated "threats to outer space…loom large" and stated a goal to "safeguard China's security interests in outer space." [153]

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.[154] More recently, US 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.[155]

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 US military superiority and protect Chinese interests.[156] 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." [157] 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.[158]

Chinese analysts assess that the US military relies upon space for 70–90 percent of its intelligence [159] and 80 percent of its communications.[160] Based on this assessment, Chinese analysts surmise that the loss of critical sensor and communication capabilities could imperil the US military's ability to achieve victory. In this context, the Chinese military seeks to deny the US military use of information from its space-based assets. Chinese military analysts have noted the dependence of the US military on space and have concluded that the loss of the use of space for the US 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.[161]

Chinese military writings state that the goal of space warfare and space operations is to achieve space superiority. Space superiority is defined a "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

153 The State Council Information Office of the People's Republic of China, "China's National Defense in the New Era," The State Council, July 24, 2019, http://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html.

154 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).

155 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.

156 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.

157 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.

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

159 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.

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

161 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.

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.[162] 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."[163] 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.[164]

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 US 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,"[165] but recommend that China should "strive to attack first at the campaign and tactical levels in order to maintain the space battlefield initiative."[166] 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."[167] In April 2022, a study sponsored by the PLA's Strategic Support Force recommended that China develop counterspace capabilities to also target commercial capabilities, such as SpaceX's Starlink broadband communications constellation in case of a future armed conflict with the United States.[168]

Chinese Space and Counterspace Organization

In recent years, China has undertaken a significant reorganization of its military space and counterspace forces. In 2015, 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.[169] 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.[170] The 2021 US Department of Defense Report on Military and Security Developments in China assessed that the SSF is responsible for the development of counterspace capabilities.[171] At this point, it is unclear if the SSF also has authority for conducting ASAT operations or whether that remains with the PLA Rocket Force.[172]

The SSF has two main function departments.[173] One of them, the Space Systems Department, handles military uses of space, including space launches, remote sensing, and the BeiDou navigation Satellites. The second department, the Network Systems Department, handles cyber operations, electronic warfare, and signals intelligence. In December 2023, new research shed light on how the SSF is organized for counterspace command and control.[174] While the report did confirm the growing role of the two Departments, it also found differences in the level of control for different counterspace capabilities and some remaining role for other services, including the PLA Air Force and Rocket Force.[175] It found that the Central Military Commission (CMC) retains control of Chinese DA-ASAT capabilities, while offensive cyber and reversible DEW dazzling counterspace capabilities are likely under the control of Theater Commanders.

162 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.

163 Ibid, p. 1.

164 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.

165 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.

166 Ibid, p. 52.

167 Ibid, pp. 142-143.

168 Stephen Chen, "Chinese researchers say China's military must be able to destroy Elon Musk's Starlink satellites in a war," South China *Morning Post*, May 25, 2022, https://www.businessinsider.com/china-need-ability-to-destroy-elon-musk-starlink-researchers-say-2022-5.

169 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/.

170 "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.

171 "Military and Security Developments Involving the People's Republic of China 2021," *U.S. Department of Defense*, p. 64, https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF.

172 Ibid.

173 Jack Lau, "China's Strategic Support Force: what do we know about the hi-tech military branch?" South China Morning Post, December 19, 2022, https://www.scmp.com/news/china/military/article/3203702/chinas-strategic-support-force-what-do-we-know-about-hi-tech-military-branch.

174 Kristin Burke, "PLA Counterspace Command and Control," China Aerospace Studies Institute, December 2023, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/PLASSF/2023-12-11%20Counter-space-%20web%20version.pdf.

175 Ibid.

The SSF does have a base dedicated to military SSA, which is known as Base 37. Base 37 is composed of units from the CMC former general departments, individual PLA services, and also civilians.[176] It is likely headquartered in Lintong City, Sha'anxi Province.[177]

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.[178] However, any estimate of China's spending and budget should be seen with a great deal of skepticism.

According to the US 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.[179] There is no public evidence that the LUOYANG exercise has been repeated. Elements of the SSF have reportedly participated in more than eleven different exercises since May 2018, although it is unclear if any of them involved space operations.[180]

176 Kristin Burke, "The PLA's New Base for Space Situational Awareness - Opportunities and Challenges for the U.S.," China Aerospace Studies Institute, September 2023, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/PLASSF/2023-09-11%20The%20PLA's%20New%20Base%20for%20SSA.pdf.

177 Burke, "PLA Counterspace Command and Control," ibid.

178 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.

179 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.

180 "PLA Aerospace Power: A Primer on Trends in China's Military, Air, Space, and Missile Forces," China Aerospace Studies Institute, 3rd Edition (August 2022), https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Other-Topics/2022-08-15%20PLA%20Primer%203rd%20edition.pdf.

28.6139°N

04

INDIA

77.2090°E

Assessment /

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 of space and creating explicit military space capabilities. India's military has developed indigenous missile defense and long-range ballistic missile programs that could lead to DA-ASAT capabilities, should the need arise. India demonstrated its ASAT capability in March 2019 when it destroyed one of its satellites and has reportedly demonstrated EW counterspace capabilities.

Specifics /

Co-Orbital ASAT

In April 2023, ISRO announced it had autonomously landed its prototype for a reusable launch vehicle, RLV-TD (reusable launch vehicle, technology demonstrator).[1] The experiment, which has been described as a space plane and looks very similar to the US' X-37B and China's Shenlong (see US Co-Orbital ASAT, Section 1.1, and Chinese Co-Orbital ASAT, Section 3.1), was taken via helicopter to an altitude of 4.5 km, released, and then was able to land by itself on a runway.[2] This was the second time this technology had been flown; the first was in May 2016, when it was launched to an altitude of 65 km via a rocket and landed in the ocean.[3] While the program has been described as developing technologies for a reusable launch vehicle and not as a counterspace capability, the possibility has been raised that it could spend up to a month in space, conducting experiments and releasing payloads; if it does eventually develop that capability, then it may have a latent counterspace capacity.

Direct Ascent ASAT

India launched its first rocket – a US-supplied Nike-Apache – in November 1963.[4] In July 1980, with the Rohini RS-1 satellite, India became the 7th nation to have indigenous satellite launch capabilities.[5]

India's space program was at first primarily focused on peaceful uses and development. However, as more countries incorporated space into security capabilities, this became more attractive to India as well. China had its first successful ASAT missile test intercept in 2007, which generated space debris and worries globally about its military space capacity. Indian officials operating in the context of historically fraught Indo-Chinese relations, including a war in 1962, ongoing border disputes, and concerns about China's role in the Asia-Pacific, began to consider whether India should have its own ASAT capability. LtGen H S Lidder, then Integrated Defense Staff chief, was quoted as saying, "[W]ith time, we will get sucked into the military race to protect space assets and inevitably there will be a military contest in space. In a life-and-death scenario, space will provide the advantage."[6]

Dr. K. Kasturirangan, former head of the Indian Space Research Organization (ISRO), said in September 2009 that "India has spent a huge sum to develop its capabilities and place assets in space. Hence, it becomes necessary to protect them from adversaries. There is a need to look at means of securing these."[7] Air Chief Marshal P.V. Naik said in February 2010, "Our satellites are vulnerable to ASAT weapon systems because our neighborhood possesses one."[8]

In February 2010, V.K. Saraswat, who at that time was the head of India's Defense Research and Development Organization (DRDO), stated, "In Agni-III, we have the building blocks and the capability to hit a satellite but we don't have to hit a satellite," due to debris concerns; instead, India "will validate the anti-satellite capability on the ground through simulation."[9] In 2012, Saraswat

1 "ISRO successfully conducts the Reusable Launch Vehicle Autonomous Landing Mission (RLV LEX), ISRO, April 2, 2023, https://www.isro.gov.in/Reusable_launch_vehicle_autonomous_landing_mission.html.

2 Jatan Mehta, "ISRO continues building its own spaceplane," *Payload Space*, April 10, 2023, https://payloadspace.com/isro-continues-building-its-own-spaceplane/.

3 Sidarth MP, "EXCLUSIVE: India lands unmanned spaceplane with pin-point accuracy; next destination is space," *WION*, April 2, 2023, https://www.wionews.com/india-news/exclusive-india-lands-unmanned-spaceplane-with-pin-point-accuracy-next-destination-is-space-578210.

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

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

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

7 "Ex-ISRO chief calls China's A-SAT a cause for worry," *Press Trust of India*, September 14, 2009.

8 Bharath Gopalaswamy and Harsh Pant, "Does India need anti-satellite capability?" *Rediff News*, February 9, 2010, http://news.rediff.com/column/2010/feb/09/does-india-need-anti-satellite-capability.htm.

9 "India has anti-satellite capability: Saraswat," *Press Trust of India*, February 10, 2010.

asserted, "Today, India has all the building blocks for an anti-satellite system in place. We don't want to weaponize space but the building blocks should be in place. Because you may come to a time when you may need it… We will not do a physical test (actual destruction of a satellite) because of the risk of space debris affecting other satellites." [10] 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 to track satellites in orbit, and noted the work done on the BMD system's communications and kill vehicles.[11] 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." [12]

India's missile defense system was intended to have two phases: one that would intercept an intermediate-range ballistic missile (IRBM), a capability that initially was planned to be in place around 2012/2013, and one that would intercept an intercontinental ballistic missile (ICBM), a capability that initially was planned to be in place around 2016. The first phase's interceptors were the Prithvi Air Defense (PAD) system (later to be replaced by the Prithvi Defense Vehicle, or PDV) and the Advanced Area Defense (AAD) system; the second phase would use the AD-1 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.[13] It was tested at night in September 2018 and was able to "successfully engage" its target.[14] The AAD was launched in March 2017 to make a successful intercept at an altitude of 15-25 km.[15] It was tested in August 2018 and successfully destroyed its target, which was surrounded by decoys.[16] In January 2020, government officials stated that the system was complete.[17] The AD-1 missile was successfully flown for the first time in a November 2022 test and is designed to be able to provide both endo- and exoatmospheric intercepts.[18] 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.[19] In April 2023, Indian military officials announced the successful first test of a sea-based endoatmospheric missile interceptor.[20] India's missile defense network uses the Swordfish long range tracking radar (see Imagery Appendix, pg. 16-56), which is a derivative of the Green Pine radar developed by Israel as part of its Arrow missile defense system.

10 Sandeep Unnithan, "India has all the building blocks for an anti-satellite capability," *India Today*, April 27, 2012, http://indiatoday.intoday.in/story/agni-v-drdo-chief-dr-vijay-kumar-saraswat-interview/1/186248.html.

11 Ibid.

12 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.

13 "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.

14 "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.

15 "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.

16 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/.

17 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/.

18 Ahmad Adil, "India conducts maiden flight-test of ballistic missile defense interceptor," Andalou Agency, Nov. 2, 2022, https://www.aa.com.tr/en/asia-pacific/india-conducts-maiden-flight-test-of-ballistic-missile-defense-interceptor/2727822.

19 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.

20 Adithya Krishna Menon, "India Conducts First Test Of New Ship-Based BMD System," Naval News, April 25, 2023, https://www.navalnews.com/naval-news/2023/04/india-conducts-first-test-of-new-ship-based-bmd-system/.

FIGURE 4-1 — MISSION SHAKTI ASAT[21]

Image Credit: DRDO

On March 27, 2019, the Indian Prime Minister Narendra Modi announced that they had successfully conducted Mission Shakti, where a KKV launched from the Kalam Island launch complex (see Imagery Appendix, pg. 16-19) 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 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. ISRO launched the satellite but did not know that it was intended to be an ASAT target, just that it was intended to have a defense application.[22] The kill vehicle's terminal guidance used a ring laser gyro-based inertial navigation system and a strap-down Imaging Infrared Seeker; the interception was done at a speed of 10 km/second, with the electro optical tracking system tracking the entire engagement.[23] 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.[24] 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."[25] 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.[26] Minister of Defence Rajnath Singh tweeted on the one-year anniversary of Mission Shakti, "The success of 'Mission Shakti'

21 Masao Dahlgren, Post on Twitter, April 19, 2021,https://twitter.com/masao_dahlgren/status/1384192441020911616.

22 Ankit Panda, Post on Twitter, April 20, 2021, https://twitter.com/nktpnd/status/1384531089901998081.

23 Dinakar Peri, "Two Years Since ASAT Test, DRDO Working on Several Key Space Technologies," *The Hindu*, March 26, 2021, https://www.thehindu.com/news/national/two-years-since-asat-test-drdo-working-on-several-key-space-technologies/article34171447.ece.

24 Indranil Roy, "All You Need To Know About The PDV MK-II: India's Satellite Killer," *Delhi Defence Review*, April 3, 2019, https://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.

25 "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.

26 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/.

proved our capability to defend the assets in outer space and made India the 4th Space Power in the world."[27]

Shortly after the test, anonymous US government sources stated that they had detected an earlier failed ASAT test in February 2019 where the PDV failed thirty seconds into flight.[28] 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 4-1 — 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 re-enter in a few days, with the entirety of it coming back down within 45 days at most.[29] 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 3.2). However, Microsat-R was at a much lower altitude when destroyed, 300 km versus 800 km for the FY-1C, meaning the orbital debris generated had a shorter lifespan. The US military cataloged 130 pieces of trackable orbital debris from India's test; the final piece of trackable debris re-entered the atmosphere in June 2022, 3.2 years after the test occurred. 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 US Direct-Ascent ASAT, Section 1.2).

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 before 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 weapon state. Successfully demonstrating its DA-ASAT capability might have been a political prerequisite for India to support discussions on a future ban.

India's main space vehicle launchpad is at Satish Dhawan Space Center near Sriharikota (see Imagery Appendix, pg. 16-18). Officials announced in August 2017 that work began on a second vehicle assembly building at the center that was anticipated to be completed by mid-2018; it was dedicated in 2019.[30] According to A S Kiran Kumar, then ISRO chairperson, "With the new assembly facility, we will be able to assemble the launch vehicle [in parallel] and bring it to existing two launchpads. It will thus help boost the launch capability of the Sriharikota center."[31] Launches from the center were initially expected to increase from seven a year to 12 a year, and in fact, 14 launches are planned for 2023, nine actually occurred.[32] Undeterred, Indian officials announced in February 2024 that they would hold 30 launches over 15 months; additionally, work has begun on a second launch facility in Tamil Nadu for private launches.[33]

27 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.

28 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/.

29 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/.

30 "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; "ISRO acquiring land in TN for its 2,300-acre second launch centre," *New Indian Express*, January 2, 2020, https://www.newindianexpress.com/nation/2020/jan/02/isro-acquiring-land-in-tn-for-its-2300-acre-second-launch-centre-2083911.html.

31 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.

32 Ibid; "Sriharikota Launch Schedule," Space Launch Schedule, last accessed Feb. 20, 2023, https://www.spacelaunchschedule.com/category/sriharikota/; "Timeline," Indian Space Research Organisation, last updated January 2, 2024, https://www.isro.gov.in/Timeline.html.

33 Andrew Jones, "India targets a surge in civil and commercial launches," *SpaceNews*, February 16, 2024, https://spacenews.com/india-targets-a-surge-in-civil-and-commercial-launches/.

Electronic Warfare

India demonstrated its EW capability against Pakistani radars and communications. It has developed several indigenous offensive EW systems, including the Samyukta and Himshakti.[34] The Himshakti is reported to have the ability to jam satellite phones; the Indian Ministry of Defence announced in March 2023 an award of $364 million (30 billion rupees) to deliver two systems to the Indian Army.[35]

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.[36] In March 2022, the Indian MoD identified 18 platforms it wanted to see industry-led design and development of; this included DEWs of 300 kw and above, so this level of power is something that they are tentatively interested in.[37] Work being done by DRDO and the Centre for High Energy Systems and Sciences (CHESS), is also reported to have yielded systems that can shoot down drones.[38] However, the targets for these weapons are aerial or electronic [39]: 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.[40] 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.[41] It will start by focusing on identifying and tracking objects in LEO up to 2000 km, but eventually is hoped to have the ability to detect objects in GEO, and is anticipated to be completed by the end of 2024 or early in 2025.[42] 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."[43] In September 2021, Air Marshal Vivek Ram Chaudhari, Vice Chief of the Indian Air Force (IAF), acknowledged that India lacks the ability to identify, observe, and track non-cooperative objects in orbit.[44] In April 2022, India and the United States signed a space situational awareness agreement to expedite sharing of SSA data.[45] Air Force Air Chief Marshall VR Chaudhari noted in June 2022 that Mission Shakti "brought to fore the need for Comprehensive Space Situational Awareness (SSA) through a robust Space Surveillance Network (SSN)."[46]

Counterspace Policy, Doctrine, and Organization

After many years of being in the works, India's cabinet office officially approved its national space policy in April 2023. Prior to its completion, the only national laws specifically dealing with space for India were its Constitution from 1950, Satellite Communications Policy from 2000, and revised Remote Sensing Data Policy from 2011. 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

34 Lt Gen (Dr) R S Panwar, "India's Space Programme: Organisations and Warfighting Potential," Future Wars, August 2, 2021, https://futurewars.rspanwar.net/indias-space-programme-organisations-and-warfighting-potential/.

35 Inder Singh Bisht, "India Procures Indigenous Electronic Warfare Systems for $364M," *The Defense Post*, March 27, 2023, https://www.thedefensepost.com/2023/03/27/india-electronic-warfare-systems/.

36 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/.

37 Sanjib Kr Baruah, "What are India's top-secret Directed Energy Weapons?" The Week, July 30, 2023, https://www.theweek.in/theweek/current/2023/07/21/what-are-indias-top-secret-directed-energy-weapons.html.

39 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.

40 "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.

41 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.

42 "ISRO's Project Netra: India's Leap into Space Situational Awareness," Indian Defence Research Wing, August 2, 2023, https://idrw.org/isros-project-netra-indias-leap-into-space-situational-awareness/.

43 Chethan Kumar, "Isro's inaugurates space object tracking centre," *Times of India*, Dec. 16, 2020, http://timesofindia.indiatimes.com/articleshow/79755718.cms.

44 "Lack of military-civil cooperation framework impeding innovation in space tech: IAF Vice Chief Vivek Ram Chaudhari," *Economic Times*, September 7, 2021, https://economictimes.indiatimes.com/news/defence/lack-of-military-civil-cooperation-framework-impeding-innovation-in-space-tech-iaf-vice-chief-vivek-ram-chaudhari/articleshow/86008913.cms?from=mdr.

45 "Readout of U.S. - India 2+2 Ministerial Dialogue," U.S. Department of Defense Press Release, April 11, 2022, https://www.defense.gov/News/Releases/Release/Article/2996350/readout-of-us-india-22-ministerial-dialogue/.

46 Krishn Kaushik, "Space-based assets can be applied for military force, says Air Force chief," Indian Express, June 15, 2022, https://indianexpress.com/article/india/space-based-assets-can-be-applied-for-military-force-says-air-force-chief-7970102/.

information.[47] India's new National Space Policy describes as its vision: "To augment space capabilities; enable, encourage and develop a flourishing commercial presence in space; use space as a driver of technology development and derived benefits in allied areas; pursue international relations, and create an ecosystem for effective implementation of space applications among all stakeholders; for, the nation's socio-economic development and security, protection of environment and lives, pursuing peaceful exploration of outer space, stimulation of public awareness and scientific quest."[48] It spells out the division of labor between the Indian government (ISRO, the Department of Space, Indian National Space Promotion and Authorization Center (IN-SPACe), and NewSpace India Limited (NSIL)) and the private sector. It does not give guidance on its national security space programs.

In October 2007, the Defence Space Vision was released, and listed intelligence, surveillance, reconnaissance, communication, and navigation as primary thrust areas.[49] In 2010, the Ministry of Defense wrote a "Technology Perspective and Roadmap" which discussed developing ASATs for "for electronic or physical destruction of satellites (2,000 km altitude above earth's surface) and GEO-synchronous orbits."[50]

In June 2010, India established an Integrated Space Cell, located in the Integrated Defense Headquarters, which is comprised of all three branches of India's armed forces.[51] The Integrated Space Cell oversaw 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."[52] There has been discussion by the Ministry of Home Affairs of a "Border Space Command," that would use space capabilities to monitor India's disputed borders.[53] 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."[54]

In September 2018 Prime Minister Narendra Modi announced the creation of a Defence Space Agency (DSA) to coordinate the space assets of the three branches of the Indian armed forces and work on space protection policies for Indian space assets; it became operational late in 2019.[55] The DSA is intended to eventually have 200 personnel assigned to it and will incorporate the Defence Satellite Control Centre and the Defence Imagery Processing and Analysis Centre.[56] It was followed by the establishment in June 2019 of the Defence Space Research Organisation, which conducts research and provides technical support to the DSA.[57] With these new organizations, India may be 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 and weaknesses in its space security in July 2019 indicates a willingness to theoretically consider using these capabilities.[58] 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.[59] Government officials asserted in March 2021 that "In the last two years, a lot of work has been done to increase [India's] capabilities in space through the development of sensors and satellites by the Space group formed within the DRDO."[60]

47 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/.

48 Indian Space Policy - 2023, 2023, p. 5, https://www.isro.gov.in/media_isro/pdf/IndianSpacePolicy2023.pdf.

49 Rajat Pandit, "Dedicated satellite for Navy by year-end," *The Times of India*, May 10, 2010.

50 Ibid.

51 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), https://www.orfonline.org/wp-content/uploads/2017/02/ORF_Space-India-2.0_NEW-21Nov.pdf.

52 Sudha Ramachandran, "India goes to war in space," *Asia Times*, June 18, 2008, https://intellibriefs.blogspot.com/2008/06/india-goes-to-war-in-space.html?m=0.

53 Rajagopalan, "Need for an Indian Military Space Policy," pp. 206-207.

54 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.

55 Ajey Lele, "Indian Space Force: A Strategic Inevitability," Space Policy, 2022, https://doi.org/10.1016/j.spacepol.2022.101526.

56 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/.

57 Ibid.

58 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/.

59 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.

60 "India increases military capabilities in space two years after Mission Shakti," ZeeNews, March 26, 2021, https://zeenews.india.com/india/india-increases-military-capabilities-in-space-two-years-after-mission-shakti-2350777.html.

In April 2023, Indian Air Force (IAF) chief Air Chief Marshal V R Chaudhari said, "In the future, instead of having purely land-based offensive systems, we should also have space-based offensive systems. It will reduce the response time...The future lies in having space-based offensive platforms."[61] He also stated, "In the future, the IAF will be called upon to take part in space situational awareness, space denial exercises or space control exercises." At the same time, India's Chief of Defence Staff Gen. Anil Chauhan stated that due to the need for India to move from "space support" to "space enhancement," it should focus on "developing dual-use platforms with a special focus towards incorporating cutting-edge technology."[62] However, it is unclear how much of these statements are leaving possibilities open to India for future efforts versus actual steps being taken at present.

India's usage of space has evolved to incorporate more investment in its domestic satellite and launch capabilities, as well as an increased emphasis on a military space capability. India has earned a significant amount of foreign exchange by launching non-Indian satellites; in December 2023, news from its parliament indicated that it had launched 397 foreign satellites in the past decade and earned $441 million from doing so.[63]

India is now using satellite technologies for strategic purposes: reconnaissance, communications, and navigations. The first satellite created specifically for the military was the GSAT-7 communications satellite, launched in August 2013.[64] 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.[65] In March 2023, the Indian MoD signed a contract for a follow-up satellite, GSAT-7B, which is supposed to be deployed by 2026.[66] With the June 2017 launch of the Cartsat 2E+ Earth observation satellite, it was reported that India had 13 satellites that are being used for military purposes.[67] 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.[68]

Potential Military Utility

India has recently made significant investments in its national security space infrastructure and capabilities and incorporated those capabilities into its military operations; furthermore, it is receiving an increasing amount of income from launching satellites for other countries.

India has demonstrated a DA-ASAT capability against a LEO satellite. However, it is likely of limited military utility: the capability is more likely to be useful as a bargaining chip or a way to publicly demonstrate that India is keeping pace with China than a militarily useful capability in a future conflict. Otherwise, India risks damaging the same environment it has invested a significant amount of resources to be able to use and benefit from. Finally, India has a nascent but still very rudimentary SSA capability, so its ability to target non-Indian satellites is unclear but probably limited. Like many other countries, India likely has counterspace EW capabilities and is developing DEW technologies that may in the future be applied in a counterspace role.

Like many other countries, India likely has counterspace EW capabilities and is developing DEW technologies that may in the future be applied in a counterspace role.

61 Rajat Pandit, "India Needs Space-based "Offensive" Weapons in Future, says IAF Chief," *Times of India*, April 30, 2023, https://timesofindia.indiatimes.com/india/india-needs-space-based-offensive-weapons-in-future-says-iaf-chief/articleshow/99878896.cms.

62 "War in Space a Possibility, Need to Develop Dual-use Platforms in that Domain: CDS Anih Chauhan," *Economic Times*, April 11, 2023, https://economictimes.indiatimes.com/news/defence/war-in-space-a-possibility-need-to-develop-dual-use-platforms-in-that-domain-cds-anil-chauhan/articleshow/99404159.cms?from=mdr.

63 Siddarth MP, "ISRO has launched 397 foreign satellites in 10 years earning USD 441 million," *WION*, December 15, 2023, https://www.wionews.com/india-news/isro-has-launched-397-foreign-satellites-in-10-years-earning-usd-157-million-670042.

64 Amit R. Saksena, "India and Space Defense," *The Diplomat*, March 22, 2014, http://thediplomat.com/2014/03/india-and-space-defense/.

65 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, https://www.orfonline.org/wp-content/uploads/2017/02/ORF_Space-India-2.0_NEW-21Nov.pdf.

66 Arvind Dhananjayan, "India's Military Satellites: The Armed Forces' Bulwarks For Communication & Surveillance!" Chanakya Forum, April 17, 2023, https://chanakyaforum.com/indias-military-satellites-the-armed-forces-bulwarks-for-communication-surveillance/.

67 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.

68 Lele, "India's Strategic Space Programme," p. 191.

05

ORBITAL DEBRIS

Created by Destructive ASAT Testing

The countries listed in the prior section have carried out more than a dozen destructive ASAT tests in space, all of which have created orbital debris that persisted long after the test itself. While some of the orbital debris from past ASAT tests has decayed from orbit, significant portions of it remain on orbit today.

The amount of orbital debris created by a destructive ASAT test depends on the nature of the event: primarily the speed of the intercept and the altitude at which it occurred, as well as the mass and structure of the target. If either the interceptor or target was in orbit when the test occurred, a significant portion of the resulting debris is likely to remain in orbit as well. The lifespan of that resulting debris is primarily a function of the altitude at which the destruction happened.

Table 5-1 below lists the known destructive ASAT testing done to date, along with the number of orbital debris tracked on orbit following the test and how much remains on orbit as of the publication of this report. Note that tracked debris generally only includes pieces larger than 10 cm in size. These tests also likely created tens of thousands of pieces of small debris (less than 10 cm) that are not tracked or cataloged but pose additional threats to other spacecraft.

TABLE 5-1 — ORBITAL DEBRIS CREATED BY ASAT TESTS IN SPACE

DATE	COUNTRY	ASAT SYSTEM	TARGET	INTERCEPT ALTITUDE	TRACKED DEBRIS	DEBRIS STILL ON ORBIT	TOTAL DEBRIS LIFESPAN
Oct. 20, 1968	Russia	IS	Cosmos 248		252	76	50+ years
Oct. 23, 1970	Russia	IS	Cosmos 373		147	35	50+ years
Feb. 25, 1971	Russia	IS	Cosmos 394		118	45	50+ years
Dec. 3, 1971	Russia	IS	Cosmos 459		28	0	3.3 years
Dec. 17, 1976	Russia	IS	Cosmos 880		127	56	45+ years
May 19, 1978	Russia	IS-M	Cosmos 970		71	64	40+ years
Apr. 18, 1980	Russia	IS-M	Cosmos 1171		45	5	40+ years
Jun. 18, 1982	Russia	IS-M	Cosmos 1375		63	59	35+ years
Sept. 13, 1985	US	ASM-135	Solwind	530 km	287	0	18+ years
Sept. 5, 1986	US	Delta 180 PAS	Delta 2 R/B		18	0	< 1 year
Dec. 26, 1994	Russia	Naryad-V?	Unknown		27	24	25+ years
Jan. 11, 2007	China	SC-19	FengYun 1C	880 km	3536	2686	15+ years
Feb. 20, 2008	US	SM-3	USA 193	220 km	175	0	1+ year
Mar. 27, 2019	India	PDV-MK II	Microsat-R	300 km	130	0	3+ years
Aug.-Dec. 2019	Russia	Cosmos 2535	Cosmos 2536		30	14	3+ years
Nov. 15, 2021	Russia	Nudol	Cosmos 1408	470 km	1807	67	Unknown
				Total	**6863**	**3133**	

2

Countries Developing Counterspace Technologies

35.2802°S

06

AUSTRA-LIA

149.1310°E

Assessment /

Australia is a relative newcomer in space, although it has long played a support role by hosting ground infrastructure for satellite communications and command and control. Recently, however, Australia has been laying the groundwork for more indigenous space capabilities, including military. It has recently started a military space organization, is building out a policy framework for its military space priorities, is putting concerted efforts and resources into building its own SSA capabilities, is examining an EW capability for its Department of Defence, and is looking into non-destructive ways in which to interfere with enemy satellites.

Specifics /

Electronic Warfare

Australia announced in July 2021 the creation of Defence Project 9358 which is intended to explore the options for a ground-based EW counterspace capability and create recommendations on next steps.[1] In March 2023, Air Vice Marshall Cath Roberts, the head of Australia's Defence Space Command, said, "I think it's a really important part of where we go to is just looking at how we can have that sort of electronic warfare-type of capability to allow us to deter attacks or certainly interfere."[2] This was part of a larger conversation about the need to have non-kinetic ways to deter impacts on Australian satellites. AVM Roberts did not give a timeline for when Australia would have those EW capabilities, other than, "As soon as I can."[3]

In October 2023, LtGen Michael Guetlein, commander of Space Force Space Systems Command, announced that Australia would be purchasing one of the US military's Counter Communications System (CCS),[4] which is an offensive electronic warfare counterspace capability (see US Electronic Warfare, Section 1.3).

Space Situational Awareness

Australia's Department of Defence launched a program in July 2020 called JP9360 (Space Domain Awareness) with the goal of combining six earlier SSA projects into one program.[5] It was reported that AUD 2 billion will be invested via this project.[6] Air Commodore Philip Gordon, Director General Air Defence and Space, noted, "SDA is absolutely critical to space control and everything we do in space. It seeks to give us an independent ability to assess and verify what's going on in space, and at the same time contribute to a broader SDA enterprise with the US and our allies."[7] It expects industry to first provide data as a service (DAAS) but later iterations ("tranches") hope to develop its own data capability and mission systems.[8]

Australia is host to several of the new sensors that contribute to the United States' SSA capacity and fill in critical geographical gaps. A C-band mechanical tracking radar originally located in Antigua was moved to Naval Communication Station Harold E. Holt near Exmouth, Western Australia (see Imagery Appendix, pg. 16-39) in March 2017.[9] The SST, a 3.5-meter telescope originally developed by DARPA, was also moved to Naval Communication Station Holt (see Imagery Appendix, pg. 16-40) to be jointly operated by the USSF's Space Delta 2 unit and the Royal Australian Air Force.[10] It imaged its first objects in March 2020 and was declared operational in September 2022.[11]

In December 2023, the United States announced that Australia and the United Kingdom had officially joined the Deep Space Advanced Radar Capability (DARC) program, and that Australia would host the first operational site.[12] DARC is an effort to develop a new set of radars to detect, track, and identify objects in deep space and consists of three geographically distributed sites

1 "Defence explores options for Space Electronic Warfare," Press release by the office of the Hon Peter Dutton MP, Minister of Defence, July 29, 2021, https://www.minister.defence.gov.au/minister/peter-dutton/media-releases/defence-explores-options-space-electronic-warfare.

2 Colin Clark, "Aussie Space Command looks to electronic warfare, other tech to deter attacks on satellites," *BreakingDefense*, March 2, 2023, https://breakingdefense.com/2023/03/aussie-space-command-looks-to-electronic-warfare-other-tech-to-deter-attacks-on-satellites/.

3 Clark, ibid.

4 Sandra Erwin, "U.S.Space Force seeks to work closer with allies in face of shared threats," *SpaceNews* October 19, 2023, https://spacenews.com/u-s-space-force-seeks-to-work-closer-with-allies-in-face-of-shared-threats/.

5 Nigel Pittaway, "JP9360 to provide a sharp focus on space," *Australian Defence Magazine*, December 16, 2021, https://www.australiandefence.com.au/defence/cyber-space/jp9360-to-provide-a-sharp-focus-on-space.

6 Gregor Ferguson, "Unified space strategy update to shape defence space R&D," The Australian, April 8, 2022, https://www.theaustralian.com.au/special-reports/unified-space-strategy-update-to-shape-defence-space-rd/news-story/ad45871956260afd722583d6001ddf54.

7 Pittaway, December 16, 2021, ibid.

8 Nigel Pittaway, "Defence rethinks space surveillance roadmap," *Australian Defence Magazine*, September 9, 2021, https://www.australiandefence.com.au/defence/cyber-space/defence-rethinks-space-surveillance-roadmap.

9 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/.

10 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/; Sandra Erwin, "Space surveillance telescope developed by the U.S. begins operations in Australia," SpaceNews, September 30, 2022, https://spacenews.com/space-surveillance-telescope-developed-by-the-u-s-begins-operations-in-australia/.

11 "Joint US-Australian Space Surveillance Telescope To Be Improved," *Australian Defence Magazine*, July 16, 2020, https://www.australiandefence.com.au/defence/cyber-space/joint-us-australian-space-surveillance-telescope-to-be-improved; Erwin, September 30, 2022, ibid.

12 "US, UK, Australia annouce trilateral Deep Space Advanced Radar Capability Initiative," United States Space Force, December 2, 2023, https://www.spaceforce.mil/News/Article-Display/Article/3604036/us-uk-australia-announce-trilateral-deep-space-advanced-radar-capability-initia/.

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16

that each have multiple transmit and receive radars meshed together (see US Space Situational Awareness Capabilities, Section 1.5).

Counterspace Policy, Doctrine, and Organization

In the July 2020 Defence Strategic Update, the Australian government identified several key issue areas it wanted to focus on in space. These include assured access to space, a satellite network to allow for independent communications, SSA capabilities (sensors and tracking), and "an enhanced space control program." On the same day, Australia's Force Structure Plan 2020 included a chapter on the space domain, and noted that "Continued investment and development of space capabilities will be required to further improve Defence's resilience and enhance a large number of space-dependent capabilities across the Joint Force." In the section about space control, it calls for a focus on space domain awareness but also notes that its plans include "the development of options to enhance ADF space control through capabilities to counter emerging space threats to Australia's free use of the space domain and that assure our continued access to space-based intelligence, surveillance and reconnaissance."

Australia's Department of Defence is undertaking a "space domain review" as part of its efforts to recognize space as a full operational warfighting domain. It is intended to be completed in March 2023.

Australia announced in May 2021 that it would be establishing an Australian Defence Force (ADF) space command that will be housed within the Royal Australian Air Force. It is intended to bring together the three branches of the Australian military with representatives of the Australian government with the goal of creating "an organisation to sustain, force-generate, operate space capabilities, and assign them to a joint operation command if needed."[13] Mel Hupfeld, chief of the air force, clarified that while there were concerns about space being contested, "this does not mean that defence encourages the militarisation of space," and that "All space operations are conducted consistent with international and domestic legal obligations."[14] In March 2022, Air Vice-Marshal Catherine Roberts, the head of the Australian Defence Force's new space command, stated, "I think the activities by China and Russia, which have been fairly well documented in the public domain, scare me … We need to accelerate the capabilities so we can deal with the threats."[15] The space command, officially established in March 2022 with about 100 personnel, is reported to be investigating irreversible and reversible ways in which to disable enemy satellites (via lasers or jamming) but will not use counterspace capabilities that create debris.[16]

Australia's Ministry of Defence intends to invest AUD $7 billion in space over the next decade.[17] This was announced in July 2020 as part of its 2020 Defence Strategic Update and 2020 Force Structure Plan and is planned to be used on developing space services and emerging space technologies.[18]

In March 2022, Australia announced the head of its space agency had begun working on a national space strategy - its Space Strategic Update, or SSU - which was intended to guide the country's space activities and priorities to the 2040s and integrate its military, commercial, and civil space efforts.[19] It is intended to take 18 months to be completed.[20]

13 Malcolm Davis, "ADF space command is the right next step for Australian space power," *ASPI The Strategist*, May 5, 2021, https://www.aspistrategist.org.au/adf-space-command-is-the-right-next-step-for-australian-space-power/.

14 "Australian military to set up space division with $7bn budget," *Australian Associated Press*, May 19, 2021, https://www.theguardian.com/australia-news/2021/may/19/australian-military-to-set-up-space-division-with-7bn-budget.

15 Jack Norton, "Russia and China give Australia's space commander the need for speed," ASPI *The Strategist*, March 23, 2022, https://www.aspistrategist.org.au/russia-and-china-give-australias-space-commander-the-need-for-speed/.

16 Norton, March 23, 2022, ibid; Daniel Hurst, "Peter Dutton says space command needed as some countries 'see space as a territory for their taking'," *The Guardian*, March 21, 2022, https://www.theguardian.com/australia-news/2022/mar/22/peter-dutton-says-space-command-needed-as-some-countries-see-space-as-a-territory-for-their-taking.

17 "Australian military," ibid.

18 Rami Mandow, "Govt. Defence Strategy Invest $7 Billion in Space," *SpaceAustralia*, July 7, 2020, https://spaceaustralia.com/news/govt-defence-strategy-invest-7-billion-space.

19 Colin Clark, "'Dancing with the gorilla': Aussies launch space strategy," *BreakingDefense*, March 4, 2022, https://breakingdefense.com/2022/03/dancing-with-the-gorilla-aussies-launch-space-strategy/.

20 Malcom Davis, "Australia needs to aim high with space strategic update," ASPI *The Strategist*, March 11, 2022, https://www.aspistrategist.org.au/australia-needs-to-aim-high-with-space-strategic-update/.

Also in March 2022, Australia released its Defence Space Strategy, which reaffirmed the AUD 7 billion to be spent on space capabilities by 2036. The strategy declared that the mission of the Australian military forces in space was to shape the space domain, deter competitor actions, and despond as necessary to assure access to space capabilities. The document lists five "lines of effort" to meet that vision:

- Enhance space capability to assure Joint Force access in a congested, contested and competitive space environment;
- Deliver military effects integrated across Whole of Government and with allies and partners in support of Australia's national security;
- Increase the national understanding of the criticality of space;
- Advance Australian sovereign space capability to support the development of a sustainable national space enterprise; and
- Evolve the Defence Space Enterprise to ensure a coherent, efficient and effective use of the space domain."

The strategy also discussed Defence's role in continuing to "identify Space Control gaps and opportunities to develop a credible Space Control capability, and space capability developers will actively seek to improve resilience of the space capabilities," noting as well, "Defence will explore options consistent with its commitment to be a responsible actor in space."

In March 2022, Australia's Defence Space Command released a "Space Power eManual." It describes itself as "the foundational Defence reference on the employment of space power, complementing and supporting all levels of Defence education and doctrine;" space power is further defined as "the total strength of a nation's ability to conduct and influence activities to, in, through and from space to achieve its objectives." Space control is described as involving "offensive and defensive operations to ensure freedom of action in space by defeating efforts to interfere with or attack Australian or allied space systems and, when directed, deny space services to a competitor," and that those activities may happen in any operating domain - that is to say, not just in space - and is made up of "offensive space control, defensive space control, space electronic warfare and the aspects of navigation warfare that deal with space based PNT."

In October 2022, Australia formally pledged not to conduct destructive DA-ASAT missile tests, as one of the growing number of signatories to the moratorium on such testing initiated by the United States.[21]

In April 2023, Australia released the public version of its Strategic Defense Review, which is a periodic assessment of defense capabilities and status that has only been done twice previously (in 1986 and 2012).[22] The review was prompted by recent changes in the strategic environment, largely driven by the continued rise of China, and political dissatisfaction with how previous Australian defense policy addressed emerging challenges. This 2023 review included significant attention to space as a new domain of operations and recommended moving space into the Joint Capabilities Group, creating a centralized development and management function for space, and building a career path for space professionals.[23]

21 "Australia advances responsible action in space," Australian Ministry for Foreign Affairs, October 22, 2022, https://www.foreignminister.gov.au/minister/penny-wong/media-release/australia-advances-responsible-action-space.

22 Lam Tran, "Unpacking Australia's 2023 *Defence Strategic Review*," Center for Strategic and International Studies, September 11, 2023, https://www.csis.org/blogs/new-perspectives-asia/unpacking-australias-2023-defence-strategic-review.

23 "National Defence Defence Strategic Review," Australian Government, April, 2023, https://www.contactairlandandsea.com/wp-content/uploads/2023/04/NationalDefence-DefenceStrategicReview.pdf.

Potential Military Utility /

Australia has made significant policy changes aimed at developing more of a national security space capability and dealing with space threats. Between creating a project to develop a ground-based EW counterspace capability and statements from Australian military officials about the importance of Australia developing that capability, it is likely that Australia will have at least an initial EW counterspace capability in the near future. Furthermore, given the amount of policy documents being generated for defense space purposes, it would appear that Australia is serious about having the option to use its nascent EW counterspace capability, so it is most likely going to be operational in some capacity. Additionally, given the investment in its SSA capabilities and physical possession of some SSA radars already, should Australia decide to target space assets for offensive measures, it is likely to have at least some inherent capacity to do so.

48.8566°N

07

FRANCE

2.3522°E

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 active defense against threats. While some French officials suggested machine guns on satellites, the actual plan calls for ground-based lasers for dazzling and satellites equipped for on-orbit inspections and also with offensive lasers. In 2021 and 2022, France carried out military exercises, codenamed "ASTERX," in outer space, testing the capabilities of its Space Command, as part of France's evolving goal to be the world's third-largest spatial power.

Specifics /

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.[1] This was part of a larger discussion about how "our allies and adversaries are militarising space… we need to act."[2] 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.

France is reported to be working on what appear to be patrolling nanosatellites (10 to 20 kg each) that would be placed in GEO.[3] "Yeux en Orbite pour un Démonstrateur Agile," or YODA, are intended to be launched in 2024 or 2025,[4] and are intended to be an RPO surveillance or inspection platform, similar to the United States' GSSAP program (see US Co-Orbital ASAT, Section 1.1). The YODA program is also framed as an early technology demonstrator program of later and bigger versions of inspector satellites that would be able to protect French military satellites by 2030.[5]

DA-ASAT Technologies

There are no known plans for France to have a DA-ASAT capability currently. 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 weapon.[6] France does maintain significant expertise in space launch vehicle and ballistic missile technology that could be the basis for a future DA-ASAT program.

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. French officials have also expressed their willingness to share technology on counterspace EW capabilities with Saudi Arabia.[7]

French authorities have also discovered multiple GNSS jammers operating near the Merville airport in March 2023, operated by unknown entities.[8]

Directed Energy

In July 2019, French Minister of Defense Florence Parly indicated the potential

1 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.

2 Ibid.

3 "The War Satellite Cometh – New Technology Definition Research Note," Space & Defence, December 7, 2021, https://spaceanddefense.io/the-war-satellite-cometh-new-technology-definition-research-note/.

4 "France's Space Commander shares lessons learned from Ukraine and future plans," Satellite Observation, February 6, 2023, https://satelliteobservation.net/2023/02/06/frances-space-commander-shares-lessons-learned-from-ukraine-and-future-plans/.

5 Comité Rochefort, "The 'Non-Identical' Twins of European Military Space (Part 1)," Defense-Aerospace.com, April 20, 2022, https://www.defense-aerospace.com/europes-non-identical-military-space-twins-1/.

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

7 AzurX, "Middle East Space Roundup: 23 to 29 July, 2023," *Middle East Space Monitor*, https://mideastspace.substack.com/p/middle-east-space-roundup-23-to-29-18b.

8 Candice Clark, "ANFR Fighting against jammers," *Resilient Navigation and Timing Foundation*, 18 July 2023, https://rntfnd.org/2023/07/21/lots-of-jammers-near-french-airport/.

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

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."[9] These lasers would "dazzle those who would be tempted to approach too close."[10] Parly said that by 2025, the first capabilities under her strategy should be ready, with the completion being achieved by 2030.[11] Further information about these efforts was revealed in April 2023 as part of the French military programming law for 2024-2030. The program to develop the laser-armed satellites is FLAMHE and there is also a companion project for ground-based lasers called BLOOMLASE.[12] France has also conducted tests of the effectiveness of existing ground-based lasers against their Spot remote sensing satellites in LEO.[13]

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 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 (see Imagery Appendix, pg 16-53 and pg. 16-54), which can see objects with radar cross sections down to 1 meter at an altitude of 400-1000 km.[14] France also has three SATAM C-band radars that are not primarily SSA sensors but do have a secondary mission to track space debris.[15] 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.[16] France also has the SPOC (Système Probatoire d'Observation du Ciel) telescope, which can do initial orbit determinations, and the TAROT system of two 25 centimeter telescopes located at the Calern Observatory (see Imagery Appendix, pg 16-55) and an 18 cm telescope at the Les Makes Observatory, which – along with the ROSACE telescope – can track objects at GEO.[17] 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.[18] COSMOS operators visited the US 18th Space Defense Squadron (which is charged with running the USSF's space domain awareness mission) in October 2022 as part of an exchange to improve SSA data sharing and operational best practices.[19]

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."[20] 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.[21] The existing French GRAVES ground-based phased array radar is intended to have a follow-up capability, which, according to Parly, "must be

9 Plowright and Benoit, ibid.

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

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

12 Xavier Pasco and Paul Wohrer, "Implementing the French Space Defence Strategy: Towards space control?," *Fondation pour la Recherche Stratégique*, June 29, 2023, https://www.frstrategie.org/en/publications/notes/implementing-french-space-defence-strategy-towards-space-control-2023.

13 Julien Lausson, "Le laser, future arme de la France pour neutraliser les satellites adverses ?," *Numerama*, June 11, 2019, https://www.numerama.com/politique/525203-le-laser-future-arme-de-la-france-pour-neutraliser-les-satellites-adverses.html.

14 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.

15 Ibid.

16 Ibid, p. 34.

17 Michael Boer, Alain Klotz, Romain Laugier, Pascal Richard, Juan-Carlos Dolado Perez, Laurent Lapasset, Agnes Verzeni, Sebastien Theron, David Coward, and J.A. Kennewell, "TAROT: A network for space surveillance and tracking operations," *ESA Space Debris Office*, proceedings of the 78th European Conference on Space Debris, Darmstadt Germany, 18-21 April 2017, June 2017, https://conference.sdo.esoc.esa.int/proceedings/sdc7/paper/382/SDC7-paper382.pdf.

18 Console, Ibid.

19 Luke Kitterman, "18 SDS, France's COSMOS integrate SDA knowledge during 'Operator Exchange'," Combined Force Space Component Command Public Affairs, October 24, 2022, https://www.spoc.spaceforce.mil/News/Article-Display/Article/3197664/18-sds-frances-cosmos-integrate-sda-knowledge-during-operator-exchange.

20 Plowright and Benoit, ibid.

21 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.

able to detect satellites 1,500 km away that are no bigger than a shoe-box."[22] Parly also said that they plan to use Ariane Group's Geotracker network in order to capture pictures of objects in GEO.[23]

Another capability being discussed is onboard cameras for future Syracuse military communications satellites that could alert satellites to oncoming threats so that the satellites can take defensive actions or maneuvers.[24] A strategy of maintaining competitiveness and autonomy internationally in the SSA domain is also being pursued by the European Union Space Surveillance and Tracking (EU SST), of which France is a key member. The EU SST has increased the budget contracted to European Industry in R&D and capabilities by 205% in 2020-2022 compared to 2018-2019.[25]

In January 2023, it was announced that the European Defence Fund had awarded a contract to a consortium for the creation of a satellite, Naucrates, that could be placed in GEO in order to do close approaches to other spacecraft there and take centimeter-level resolution images.[26] Delivery of Naucrates is anticipated for 2026.[27] Presumably France, as a member of the European Commission, could get access to the SSA data generated by this satellite. In April 2023, CNES announced that it had selected a consortium led by ArianeGroup to develop a network of ground telescopes and a space-based sensor to augment its existing SSA capabilities.[28]

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."[25] 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."[30] 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.[31] 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."[32] CDE is moving its offices to Toulouse to be co-located near CNES (Centre national d'études spatiales), France's civil space agency; NATO's Centre of Excellence for Space is intended to be in Toulouse as well.[33]

The French military had originally put aside 3.6-billion Euros (roughly USD 4 billion) to invest in its satellites from 2019-2025.[34] Parly announced in July 2019 an additional 700 million Euros for this effort.[35] These 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 as a result of increased missile threats.

In July 2019, France also announced its first Space Defense Strategy.[36] It has

22 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/.

23 Hitchens, July 26, 2019, ibid.

24 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.

25 "3rd EU SST Webinar: Building the future of SST," Webinar, European Union Space Surveillance and Tracking (EU SST), October 5, 2021, https://www.eusst.eu/wp-content/uploads/2021/10/3rd_EU_SST_Webinar_presentation.pdf.

26 "AAC Clyde Space To Be Part Of First European Space Situational Awareness GEO Satellite," AAC Clyde Space press release, January 26, 2023, https://investor.aac-clyde.space/en/press-releases/aac-clyde-space-to-be-part-of-first-european-space-situation-101796.

27 "AAC Clyde Space," ibid.

28 Rachel Jewett, "ArianeGroup consortium to lead French space situational awareness project," *Satellite Today*, April 24, 2023, https://www.satellitetoday.com/government-military/2023/04/24/arianegroup-consortium-to-lead-french-space-situational-awareness-project/.

29 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.

30 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-national-day-defence/france-to-create-space-command-within-air-force-macron-idUSKCN1U80LE.

31 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.

32 Ibid.

33 "France's Space Commander shares lessons learned from Ukraine and future plans," *Satellite Observation*, February 6, 2023, https://satelliteobservation.net/2023/02/06/frances-space-commander-shares-lessons-learned-from-ukraine-and-future-plans/.

34 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.

35 «France to create space command within air force: Macron,» *Reuters*, July 13, 2019, https://www.reuters.com/article/us-france-national-day-defence/france-to-create-space-command-within-air-force-macron-idUSKCN1U80LE.

36 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.

two goals: to increase and strengthen SSA for there to be better decision-making nd 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."[37] 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."[38]

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."[39] It also stated that a "consolidated assessment of threats affecting our capabilities" will be needed.[40] France's Defense Innovation Agency is 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."[41] 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."[42]

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."[43]

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.[44] 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. In February 2022, France's Space Operations Law was modified to reflect its military space strategy, allowing civilian assets to be transferred to the Ministry of Defence, designated the Ministry of Defence to be liable if those assets caused any damage, and permitted the Ministry of Defence to commandeer civilian assets.[45]

During a December 2021 hearing, French military officials announced their plans to spend EUR 646 million on space in 2022, and that they earmarked EUR 5.3 billion for military space capabilities and services to be spent between 2019 and 2025.[46]

In 2021, the French Ministry of Defense legally conducted its first military exercises in outer space.[47] The exercise was codenamed "ASTERX," and it tested the capabilities of France's Space Command in tackling 18 different space events and threats to its satellites and defense equipment.[48] ASTERX was held in 2022 as well; this version simulated 16 events and an orbital population of

37 Laudrain, ibid.

38 Hitchens, ibid.

39 Space Defence Strategy, pp. 12-13.

40 Ibid.

41 Ibid, p. 26.

42 Ibid, p. 27.

43 Ibid.

44 Philippe Clerc, "Can national space law offer solutions ? The French Space Operations Act's contribution," presentation to the Toulouse Space Show 2012, June 26, 2012, https://iislweb.space/wp-content/uploads/2020/01/2012_Clerc.pdf.

45 Stromgade on Twitter, March 9, 2022, https://twitter.com/stromgade/status/1500407634192654337?s=21; Ordinance No. 2022-232 of February 23, 2022 on the protection of national defense interests in the conduct of space operations and the use of data of space origin, Government of France, taken from the official journal Lois et Décrets vol. 47, published February 25, 2022, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045222114.

46 Vivienne Machi, "France puts space at top of national — and European — security priorities," Defense News, March 14, 2022, https://www.defensenews.com/space/2022/03/14/france-puts-space-at-top-of-national-and-european-security-priorities/.

47 "France conducts first military exercises in space," *Deutsche Welle* (DW), March 10, 2021, https://www.dw.com/en/france-conducts-first-military-exercises-in-space/a-56821868.

48 Murielle Delaporte, "ASTERX 2021: French Space Forces Reach for Higher 'Orbit,'" *BreakingDefense*, April 9, 2021, https://breakingdefense.com/2021/04/asterx-2021-french-space-forces-reach-for-higher-orbit/.

10,000 objects.[49] It was broader in terms of scope from the previous year's exercise in that it included the European External Action Service (EEAS) plus four other countries; it also incorporated commercial data via the Commercial Integration Cell (CIC).[50]

In November 2022, France formally pledged not to conduct destructive DA-ASAT missile tests, as one of the growing number of signatories to the moratorium on such testing initiated by the United States.[51]

Potential Military Utility /

Between the SAMP/T missile defense system and its extensive space launch and ballistic missile expertise, France has the technological building blocks to develop a DA-ASAT capability if it chooses to do so, although there are no indications it has such plans. France is developing the initial capability for ground-based DEW and RPO satellites armed with DEW in GEO that may enable a future co-orbital ASAT program, but it is unclear whether they will be capable of just temporary dazzling or doing more permanent damage to other satellites. Additionally, France's indigenous SSA capabilities are fairly well-developed so they could potentially be used for targeting non-French satellites and could be of limited military utility as well. Finally, given the amount of policy documents and military space organization being generated for defense space purposes, it would appear that France is serious about using counterspace capabilities, once they are more solidly developed.

49 "ASTERX 22: France's annual military space exercise," SatelliteObservation.net, March 6, 2022, https://satelliteobservation.net/2022/03/06/asterx-22-frances-annual-military-space-exercise/.

50 "ASTERX 22," ibid.

50 "Space - France's commitment not to conduct destructive direct-ascent anti-missile tests (29 November 2022)," Ministere Del L'Europe Et Des Affaires Etrangeres, November 29, 2022, https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/news/2022/article/space-france-s-commitment-not-to-conduct-destructive-direct-ascent-anti.

35.6892°N

08

IRAN

51.3890°E

Assessment /

Iran has a nascent space program, 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 motivation for doing so at this point. Iran's military appears to have an independent ability to launch satellites, separate from Iran's civil space program. Iran has not demonstrated any ability to build homing kinetic kill vehicles, and its ability to build nuclear devices is still constrained. Iran has demonstrated an EW capability to persistently interfere with the broadcast of commercial satellite signals, although its capacity to interfere with military signals is difficult to ascertain.

Specifics /

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, starting with liquid-fulled SLVs like the Safir and Simorgh, but it has had recent success with mix- and solid-fuelled SLVs built by the IRGC like the (respectively) Qassed and Qaem-100. Its pace of launch attempts was slow, possibly due to sanctions on its ability to make progress, or perhaps because it is sensitive to international reaction to satellite launches because of their similarities to ballistic missile launches, but it has seen an uptick over the past year, both in launch attempts and successes.

Iran has successfully launched eight satellites into orbit. They have all been small satellites, 50 kilograms or lighter, lofted into such low-altitude orbits that atmospheric drag brought them down fairly quickly. No data has 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,[1] both developed domestically and through bilateral cooperation with other countries, but many of those plans have been significantly delayed. Russia launched a remote sensing satellite ("Khayyam") for Iran in August 2022; Iranian officials say that the satellite is intended to conduct environmental monitoring and scientific research.[2] Russia is also thought to be working on a geostationary communications satellite, "Ekvator;" while it is not clear that Iran is the customer, its slot is 34 degrees east longitude, which according to the International Telecommunication Union (ITU) is a slot that is reserved for an Iranian communication satellite.[3] Iran first announced that it would attempt to launch its Nahid-2 communications satellite before the end of 2018, then said in February 2023 that it and two other satellites (Toulou-3 and Zafar) would be launched by May 2023; as of February 2024, they have not been launched.[4] 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), which would be necessary to develop an effective co-orbital ASAT capability.

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

1 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.

2 "Russia puts Iranian satellite into orbit," *Reuters*, August 9, 2022, https://www.reuters.com/world/russia-launches-iranian-satellite-into-space-under-shadow-western-concerns-2022-08-09/.

3 Bart Hendrickx, "Russia and Iran expand space cooperation," *The Space Review*, October 31, 2022, https://www.thespacereview.com/article/4475/1.

4 "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; "Iran Sends 3 Research Devices into Space Successfully," *Farsi News Agency*, December 30, 2021, https://www.farsnews.ir/en/news/14001009000505/Iran-Sends-3-Research-Devices-in-Space-Sccessflly; "Iran unveils Nahid-2, Tolou-3 homegrown satellites," ***Xinhua News Agency***, February 7, 2023, https://english.news.cn/20230207/d965a36c7a384e27b708496bfc82e14d/c.html.

status or in development, with estimated ranges from 150 km to more than 2,000 km. The longer-range missiles could theoretically be used as the basis for a DA-ASAT rocket, with a potential ceiling of roughly 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.[5] However, many other experts discount the ability to use a primitive nuclear device in this way,[6] and state that this is a scare tactic designed to promote missile defense.[7]

Iran is also developing several different space launch capabilities, both civil and military. Its first space launch vehicle was the Safir rocket, which was used to successfully place four small satellites into orbit (on four different flights) from the Semnan Space Launch Complex (see Imagery Appendix, pg. 16-20). Iran has also develop a more capable SLV known as the Simorgh, which had a troubled development. Simorgh shares some design similarities with the North Korean Unha SLV and was initially meant to have been launched in 2010.[8] In April 2016, the first known test of the Simorgh was reported by US intelligence agencies to have been a "partial success" that did not reach orbit.[9] A second test in July 2017 was reported by Iranian press to have been a success, but US intelligence officials stated it was a catastrophic failure and no objects reached orbit.[10] Iran held a Simorgh launch in January 2019 which failed to launch its satellite, Payem.[11] 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."[12] An unsuccessful space launch was detected by US military analysts in June 2021; it is unclear what rocket was used, but it is possible that it was a Simorgh. A second launch may have been held at that same launch pad later that month, possibly of a Simorgh again.[13] In December 2021, Iran launched a Simorgh with three payloads on-board, none of which appear to have made it to orbit.[14]

A successful launch of the Simorgh SLV finally occurred in January 2024, when a Simorgh lifted three satellites to an altitude of 450 km. Two cubesats, Kayhan-2 and Hatef-1, are intended to test narrowband communication and geopositioning technology. A larger third satellite, Mehda, is described as a "research satellite" intended to help the ISA ascertain how well the Simorgh is at placing objects in orbit.[15]

In addition to the civil SLVs being developed by the Iranian Space Agency, the Iranian military is also developing their own SLV that has shown more success. 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 (see Imagery Appendix, pg. 16-21), 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).[16] 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).[17] The same day that

5 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.

6 Philip Bump, "Republican Warnings About an Electro-Magnetic Pulse (EMP) Attack, Explained," *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.

7 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/.

8 Center for Strategic and International Studies, "Simorgh," *Missile Threat*, accessed March 21, 2018, https://missilethreat.csis.org/missile/simorgh.

9 Bill Gertz, "Iran Conducts Space Launch," *Washington Free Beacon*, April 20, 2018, http://freebeacon.com/national-security/iran-conducts-space-launch/.

10 "Iran Announces First Successful Simorgh Test Launch," *SpaceFlight101.com*, July 29, 2017, http://spaceflight101.com/iran-announces-first-successful-simorgh-test-launch/.

11 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.

12 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.

13 William Graham, "Iran's Simorgh rocket falls short of orbit with three payloads aboard," *NASASpaceflight.com*, December 30, 2021, https://www.nasaspaceflight.com/2021/12/iran-simorgh-three-payloads/.

14 Graham, December 30, 2021, ibid.

15 Brett Tingley, "Iran launches 3 satellites on Simorgh rocket's 1st successful orbital launch," *Space.com*, January 29, 2024, https://www.space.com/iran-satellite-launches-middle-east-conflicts-january-2024; "Iran launches three satellites amid rising tensions with Western powers," *Al Jazeera*, January 28, 2024, https://www.aljazeera.com/news/2024/1/28/iran-launches-three-satellites-amid-rising-tensions-with-western-powers; Gunter D. Krebs, "*Simorgh (Safir-2)*", Gunter's Space Page, Retrieved February 22, 2024, from https://space.skyrocket.de/doc_lau/simorgh.htm.

16 Hinz, ibid.

17 Hinz, ibid.

the Salman motor footage was released, Iranian news reported that a solid fueled SLV, the Zuljanah, was finished and would be able to launch the Nahid I satellite, potentially as early as June 2020.[18]

Footage of the launch of the Zuljanah rocket was aired on Iranian television in February 2021; it did not attempt to put a satellite in orbit, but Iranian defense ministry officials who oversaw the program stated that it could carry one 220 kg-sized satellite or 10 smaller ones.[19] Satellite imagery in February 2022 showed the aftereffects of an apparent explosion at the Imam Khomeini Spaceport; the damaged gantry resembled the one used for launching the Zuljanah satellite launch vehicle in 2021.[20] Reports emerged in June 2022 that Iran had launched the Zuljanah SLV but it is unclear when the launch occurred; again, the Zuljanah did not appear to be carrying any satellites.[21]

In April 2020, the IRGC launched from its Shahroud base a satellite (Noor-1) on a previously unknown SLV, the Qassed.[22] 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; the Qassed 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 an SSO at an altitude of 425 km and it eventually deorbited in April 2022.[23] Ali Jafarabadi, head of IRGC's space force, announced in June 2020 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.[24]

In January 2022, the IRGC reported that it launched a solid-fueled rocket for the first time.[25] The IRGC successfully launched Noor-2 on the Qassed SLV to an altitude of 500 km in March 2022; this marked the second military satellite in orbit for Iran.[26] The third military satellite for Iran, Noor-3, was launched in September 2023, also on a Qassed SLV; this is thought to be an imaging satellite and has been tracked to an altitude of about 450 km.[27]

The IRGC successfully launched a new three-stage, solid-fueled SLV called the Qaem-100 in November 2022 in a test flight that was suborbital.[28] In January 2024, the IRGC used the Qaem-100 to place the 50-kg Sorayya satellite into an altitude of 750 km, reported to be the highest altitude yet reached by an Iranian satellite.[29] The IRGC announced after the Sorayya was launched that it intended to test another new SLV, the Qaem-105, within the next year, and the Qaem-120 within three years; the Qaem-120 is planned to allow Iran to reach GEO.[30]

Iran is anticipated to start work on a new launch base at Chabahar, along its southeastern coast, which may become Iran's primary launch site; Iranian officials say that the initial design and construction phase will be completed by March 2025, and that it will be completely operational and capable of launching international payloads by 2031.[31]

18 Hinz, ibid.

19 Nasser Karimi, "Iran state TV airs launch of new satellite-carrying rocket," *The Associated Press*, February 1, 2021, https://apnews.com/article/space-launches-middle-east-iran-46fef0c23da4a42e5aae42daf00fe887.

20 Jon Gambrell, "Satellite photos show Iran had another failed space launch," *The Associated Press*, March 2, 2022, https://apnews.com/article/space-launches-technology-science-business-iran-4ed71f17a612e8aef2c9b58af4538183.

21 "Iran Reports Test Of Satellite Launcher As Diplomats Announce Restart Of Nuclear Talks," *RFE/RL*, June 26, 2022, https://www.rferl.org/a/iran-satellite-launcher-test-zuljanah/31915794.html.

22 "Iran's Military Satellite Launch Full Of Surprises," *SpaceWatchGlobal*, April 2020, https://spacewatch.global/2020/04/irans-military-satellite-launch-full-of-surprises/.

23 "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/; Mike Wall, "Iran launches 3rd military satellite to orbit," *Space.com*, September 28, 2023, https://www.space.com/iran-launches-noor-3-imaging-satellite-september-2023.

24 Khosro Kalbasi, June 8, 2020, https://twitter.com/KhosroKalbasi/status/1269971351475011584.

25 "Report: Iran launched solid-fuel satellite rocket into space," *Associated Press*, January 13, 2022, https://abcnews.go.com/International/wireStory/report-iran-launched-solid-fuel-satellite-rocket-space-82245006.

26 "Report: Iran's Revolutionary Guard launches second satellite," *Al Jazeera*, March 8, 2022, https://www.aljazeera.com/news/2022/3/8/report-irans-revolutionary-guard-launches-second-satellite.

27 Mike Wall, "Iran launches 3rd military satellite to orbit," *Space.com*, September 28, 2023, https://www.space.com/iran-launches-noor-3-imaging-satellite-september-2023.

28 "Launch of Qaem satellite-carrying rocket made foes angry, delirious: diplomat," *Tehran Times*, November 7, 2022, https://www.tehrantimes.com/news/478449/Launch-of-Qaem-satellite-carrying-rocket-made-foes-angry-delirious.

29 "Iran successfully launches Sorayya satellite, state media report," *Reuters*, January 20, 2024, https://www.reuters.com/world/middle-east/iran-successfully-launches-sorayya-satellite-iranian-media-2024-01-20/.

30 Nigar Bayramli, "Iran Successfully Launches Three Satellites Simultaneously Using Domestic Satellite Launch Vehicle," *Caspian News*, January 29, 2024, https://caspiannews.com/news-detail/iran-successfully-launches-three-satellites-simultaneously-using-domestic-satellite-launch-vehicle-2024-1-29-0/.

31 Lamson and Lewis, ibid; "Iran's Chabahar Space Center to be completed by March 2025," *Al Mayadeen English*, September 11, 2023, https://english.almayadeen.net/news/technology/irans-chabahar-space-center-to-be-completed-by-march-2025.

FIGURE 8-1 — IRANIAN BALLISTIC MISSILES

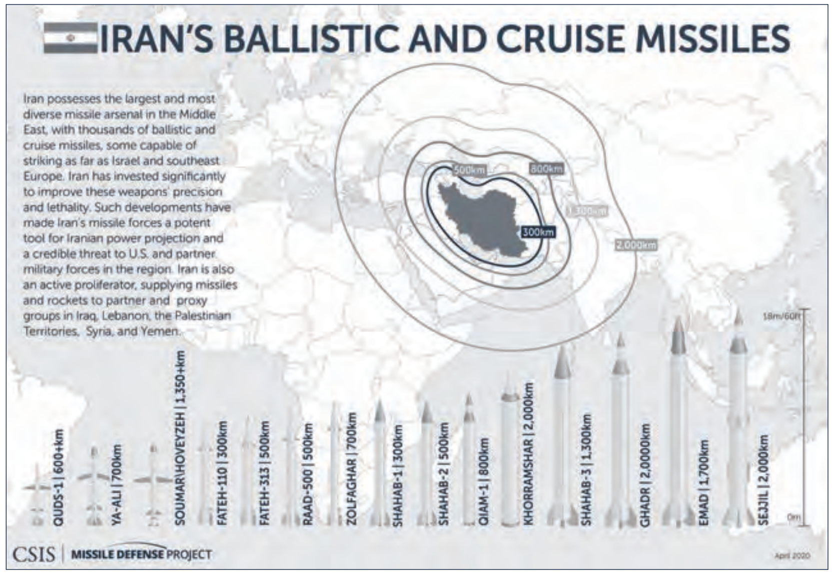


Image Credit: CSIS [32]

Electronic Warfare

There is significant public evidence that Iran could conduct electronic warfare attacks against commercial satellite broadcasters. Specifically, Iran has 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.[33] Eventually, it appears, Iran became able to jam these channels from within its own territory.

In 2010, the 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.[34] Eutelsat stated in October 2022 that two of its satellites were undergoing jamming from transmissions originating in Iran.[35]

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 US RQ-170 Sentinel UAV landed in Iran.[36] The United States confirmed that a UAV had landed in Iran and asked for its return.[37] 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 the UAV 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,

32 Center for Security and International Studies, "Iran's Ballistic Missiles," *Missile Threat*, accessed March 21, 2018, https://missilethreat.csis.org/country/iran/.

39 Peter B. de Selding, "ITU Implores Iran to Help Stop Jamming," *SpaceNews*, March 26, 2010, https://spacenews.com/itu-implores-iran-help-stop-jamming/.

40 Jason Rainbow, "Eutelsat says satellite jammers within Iran are disrupting foreign channels," Space News, October 7, 2022, https://spacenews.com/eutelsat-says-satellite-jammers-within-iran-are-disrupting-foreign-channels/.

36 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.

37 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.

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 base in Afghanistan.[38] While the ability to conduct such a spoofing attack on the civil GPS signal has been demonstrated,[39] conducting a similar attack on the military GPS signal would be much more challenging because it is encrypted. It is possible that Iran may have found a way to jam the military GPS signal, forcing the UAV to fall back on the civil signal. After the capture of the sophisticated drone, Iran claims it had 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.[40]

In August 2019, the US government issued public warnings to commercial shipping about potential Iranian jamming and spoofing of space services.[41] The warning cites several incidents of ships reporting GPS interference, bridge-to-bridge communications spoofing, and/or other communications jamming.[42] Unnamed US 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 US 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.[43] There was another incident of circle spoofing detected by the fitness app Strava around an Iranian government facility in Tehran.[44]

In September 2023, there were numerous reports of commercial airlines losing their navigation systems when flying in the Middle East, with their GPS information being spoofed so that they thought they were somewhere other than they actually were, causing some to fly off-course.[45] The source of the spoofing was traced to outside of Tehran. In some cases, it was also reported that the planes' Inertial Reference Systems (IRS), which are supposed to serve as back-ups to GPS, were also corrupted by the spoofing.

Space Situational Awareness

Iran is developing some SSA capabilities that in theory could eventually be used to track targets and be used in future counterspace capabilities, but currently appear to be very limited in capability and coverage. In 2013, a center in Delijan (see Imagery Appendix, pg. 16-57) was opened that was intended to provide Iran with space object monitoring capabilities via electro-optical, radar, and radio methods.[46] 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.[47]

Counterspace Policy, Doctrine, and Organization

The IRGC announced in April 2020 the existence of its Aerospace Force's Space Command.[48] Iranian President Ebrahim Raisi has also recently put a lot of emphasis on Iran's space program. He chaired a meeting of the Supreme Space Council in 2021 (which had not convened in over a decade), where he said that Iran would be able to reach GEO by 2026.[49] The meeting also resulted in a launch schedule going through March 2023 to deal with some of the backlog of Iranian satellites waiting to be launched.[50] In February 2023, it was reported that the Raisi administration wishes to turn Iran into an exporter of space technology services within a year or the end of the Raisi administration,

38 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/.

39 "Spoofing a Superyacht At Sea," *UT News*, July 30, 2013, https://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea/.

40 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/.

41 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/.

42 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.

43 Dana Goward, "GPS Circle Spoofing Discovered In Iran," *GPS World*, April 21, 2020, https://www.gpsworld.com/gps-circle-spoofing-discovered-in-iran/.

44 Goward, April 21, 2020, ibid.

45 Matthew Gault, "Commercial Flights Are Experiencing 'Unthinkable' GPS Attacks and Nobody Knows What to Do," *Vice.com*, November 20, 2023, https://www.vice.com/en/article/m7bk3v/commercial-flights-are-experiencing-unthinkable-gps-attacks-and-nobody-knows-what-to-do.

46 "Iran Opens New Space-Tracking Center," *RFE-RL*, June 9, 2013, https://www.rferl.org/a/iran-space-tracking-center/25011651.html.

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

48 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/Ibid.

49 Jim Lamson and Jeffrey Lewis, "Iranian President Raisi's Renewed Emphasis on Space is Likely to Create New Tensions," *War on the Rocks*, December 20, 2021, https://warontherocks.com/2021/12/iranian-president-raisis-renewed-emphasis-on-space-is-likely-to-create-new-tensions/.

50 Lamson and Lewis, ibid.

again, demonstrating the government's continued interest in enhancing its domestic space capabilities.[51]

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 destructive 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 can 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 US 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.[52]

51 "Iran plans to turn into exporter of space-related services: Min.," Islamic Republic News Agency, February 7, 2023, https://en.irna.ir/news/85022430/Iran-plans-to-turn-into-exporter-of-space-related-services-Min.

52 "Collateral Damage to Satellites from an EMP Attack," *Defense Threat Reduction Agency*, August 2010, https://apps.dtic.mil/dtic/tr/fulltext/u2/a531197.pdf.

32.08°N

09

ISRAEL

34.78°E

Assessment /

In 1988, Israel became the eighth country to be able to launch its own satellite into orbit. It has maintained a space program that has largely been civil in nature and co-developed a missile defense system that has been until recently strictly for endoatmospheric interception of rockets. However, in recent years Israel has moved to expand its military space program and there's evidence it has developed counterspace capabilities. These include the recent demonstration of an exoatmospheric missile defense intercept capability and use of EW in active military conflicts. It is possible that Israel has additional counterspace capabilities that are not publicly visible or documented.

Specifics /

DA-ASAT Technologies

Israel has never tested a DA-ASAT weapon or had an explicit DA-ASAT development program, but likely has an inherent DA-ASAT capability from part of its ballistic missile defense system. The Arrow-3, which is co-developed by the Israel Missile Defense Organization (IMDO) and the US Missile Defense Agency (MDA), is the most viable platform. In 2009, Yitzhik Ben-Israel, then chairman of the Israel Space Agency, noted that "If there's a threat from space, a logical answer is the Arrow upper tier" missile defense system.[1]

While the exact capabilities of the Arrow-3 in a counterspace role are unknown, it reportedly achieved an exoatmospheric intercept for the first time in November 2023 when it was used to intercept a long-range missile fired from Houthi-controlled Yemen.[2] It is unclear at what altitude the intercept was made, only that it was likely above 100 km. The Arrow-3's range suggests that it can theoretically intercept targets up to 1200 km. However, its ability to track and target objects at that level is unknown and undemonstrated.[3]

Electronic Warfare

There have been reports of interference with aircraft navigation systems for years in the eastern Mediterranean region. In spring 2023, these included reports of GPS jamming occurring over Israel and the eastern Mediterranean region, with Israeli EW systems reportedly bringing down at least one Iranian drone.[4] In April 2023, there was a particularly high level of GPS interference with aircraft guidance systems: 20 percent of civilian aircraft flying in the region reported interference with their navigation systems.[5]

After the Hamas surprise attack in Southern Israel on October 7, 2023, the amount of jamming activities in the region increased quickly, with a focus on GPS interference and jamming of communications networks. It is hard to distinguish from open sources whether the EW is being conducted by Israel, Hamas, or potentially other actors.[6] The GNSS interference was degraded to the point where air traffic into Ben Gurion Airport in Israel had slowed considerably due to flight safety concerns.[7] As the war has progressed, the Israeli Defense Forces (IDF) have stated publicly that it was jamming GPS in the region "in a proactive manner for various operational needs. Citizens should be aware that the disruption can cause various and temporary effects on location-based applications."[8] Pilots were reported to have been warned not to depend on GPS when landing in Israel.[9] The GPS interference was reported to be both jamming and spoofing.

Directed Energy Weapons

Israel is developing a high-energy laser weapon called "Iron Beam," that is part of its Iron Dome defense system. The Iron Beam is a 100 kw laser that is intended to be used against air-breathing threats. It is unclear whether Iron

1 Barbara Opall-Rome, "Israeli Experts: Arrow-3 Could Be Adapted for Anti-Satellite Role," *SpaceNews*, November 9, 2009, https://spacenews.com/israeli-experts-arrow-3-could-be-adapted-anti-satellite%E2%80%82role/.

2 Tzally Greenberg, "Israel announces first Arrow-3 operational intercept," *C4ISRNet*, November 10, 2023, https://www.c4isrnet.com/battlefield-tech/space/2023/11/10/israel-announces-first-arrow-3-operational-intercept/.

3 Timur Kadyshev, "An Analysis [of] the Utility of Arrow 3 for European Missile Defense," MIT Global Security Technical Webinar Series, February 6, 2024.

4 Avi Scharf, "GPS Jamming in Israel Spikes Amid Regional Flare-up," *Haaretz*, April 10, 2023, https://www.haaretz.com/israel-news/security-aviation/2023-04-10/ty-article/.premium/gps-jamming-in-israel-spikes-amid-recent-flareup/00000187-6589-dcdb-a9af-eda9f9330000.

5 Ibid.

6 Dean Mikkelsen, "GPS jamming escalates amid Israel-Hamas conflict," *Defense and Security Middle East*, October 10, 2023, https://www.defsecme.com/defence/tech/gps-jamming-escalates-amid-israel-hamas-conflict.

7 Jesse Khalil, "GPS jamming increases amid Israel Hamas conflict," *GPS World*, October 11, 2023, https://www.gpsworld.com/gps-jamming-increases-amid-israel-hamas-conflict/.

8 Avi Scharf and Yaniv Kubovich, "Israel Ramps Up GPS Jamming to Thwart Hezbollah, Hamas Drone Attacks," *Haaretz*, October 11, 2023, https://www.haaretz.com/israel-news/security-aviation/2023-10-16/ty-article/.premium/israel-ramps-up-gps-jamming-to-thwart-hezbollah-hamas-drone-attacks/0000018b-3784-d051-a1cb-3fdfdfe10000; IDF Real Time Updates, October 15, 2023, https://www.idf.il/en/mini-sites/hamas-israel-war-24/real-time-updates/.

9 Matt Berg, "Israel's using widespread GPS tampering to deter Hezbollah's missiles," *Politico*, October 23, 2023, https://www.politico.com/news/2023/10/23/israels-gps-tampering-deter-hezbollahs-missiles-00123026.

Beam could be used against exo-atmospheric targets for dazzling purposes, given it is said to have a range of a few kilometers.[11] It is unclear if Israel has other DEW capabilities that are or may be used in counterspace role in the future.

Space Situational Awareness

Israel has limited SSA capabilities that are primarily derived from its ELM-2080 Green Pine missile defense radar.[12] The system was developed as part of the Arrow missile defense system and is known to have a range of 500-900 km, which could be used to track objects in LEO.[13] Versions of the radar have been exported to India (see India Space Situational Awareness, Section 4) and South Korea (see South Korean Space Situational Awareness, Section 12).

The United States and Israel signed an SSA sharing agreement in 2015, but it appears more to have been a way to "streamline the process for USSTRATCOM partners to request specific information gathered by its Joint Space Operations Center;" it is unclear if SSA information is shared in both directions between the United States and Israel.[14]

Counterspace Policy, Doctrine, and Organization

The Space and Satellite Administration was created within the Israeli Ministry of Defense in the 1980s, while the Israeli Space Agency was created in 1983 and operates within its Ministry of Science and Technology.[15] The focus by the Israeli government agencies is on scientific research and development for economic benefit, as well as ensuring Israel's national security is strengthened. The chair of Israel Aerospace Industries (IAI), Boaz Levy, stated in a May 2023 interview that "Israel is working on space warfare capabilities;" he went on to say, "This is an area in which all the superpowers are investing, and if you ask me if I see it happening – then yes, I see it happening, but I don't know when it will happen." [16] IAI is owned by the Israeli government but it is not clear that he was speaking for the Israeli government.

While Israel has been working on national legislation regarding space, it is still in draft form.[17]

Potential Military Utility /

Israel's current counterspace capabilities appear focused on electronic warfare and interference with navigation systems — reversible and temporary in nature — and are being used in an active military conflict. While it has a theoretical DA-ASAT capability with its Arrow-3 missile defense system, it has not been tested in that capacity.

10 Mikayla Easley, "Israeli-Made High-Energy Laser Makes Debut," *National Defense*, March 21, 2023, https://www.nationaldefensemagazine.org/articles/2023/3/21/israeli-made-high-energy-laser-makes-debut.

11 "Iron Beam High Energy Laser Weapon System," *Rafael*, accessed February 29, 2024, https://www.rafael.co.il/worlds/land/iron-beam/.

12 ELM-2080 Green Pine Radar," *IAI*, accessed March 1, 2024, https://www.iai.co.il/p/elm-20802080s-green-pine.

13 "Green Pine Radar (Israel)," Missile Defense Advocacy Alliance, accessed on February 26, 2024, https://missiledefenseadvocacy.org/defense-systems/green-pine-radar-elm-2080-israel/.

14 "U.S. Strategic Command signs space data-sharing agreement with Israel," US Strategic Command Public Affairs, August 12, 2015, https://www.stratcom.mil/Media/News/News-Article-View/Article/983672/us-strategic-command-signs-space-data-sharing-agreement-with-israel/.

15 "Space and Satellite Administration," Copyright Israeli Ministry of Defense 2018, https://english.mod.gov.il/About/Innovative_Strength/Pages/Space_and_Satellite_Administration.aspx; "About the Israeli Space Agency," Accessed February 11, 2024, https://www.space.gov.il/en/about.

16 Yoav Limor, "'Israel is working on space warfare capabilities'," *Israel Hayom*, May 3, 2023, https://www.israelhayom.com/2023/05/03/israel-is-working-on-space-warfare-capabilities/.

17 "Israel's Statement to the LSC 2023 under General exchange of views," Israel, Item 3, at United Nations Committee on Peaceful Uses of Outer Space Legal Subcommittee Meeting,March 22, 2023, https://www.unoosa.org/documents/pdf/copuos/lsc/2023/Statements/22_AM/3_Israel_22Mar_AM.pdf.

35.6762°N

10

JAPAN

139.6503°E

Assessment /

Japan has long been a well-established space actor and its space activities have historically been 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 the development of enhanced SSA capabilities to support military and civil applications. While Japan does not have any acknowledged offensive counterspace capabilities, it is 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 /

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.[1] The goal would be to decide in the coming fiscal year so that if Japan decided to go ahead with such a capability, it could be launched by the mid-2020s. 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."[2] 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.[3] It is not known whether this future counterspace capability will be defensive or offensive.

DA-ASAT Technologies

Japan has no designated DA-ASAT systems under development or in operation. However, it does have the 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 US Direct-Ascent ASAT, Section 1.2). 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.[4] Japan is also working with the United States on the 3rd stage rocket motor and nose cone of the SM-3 Block IIA interceptor, which is intended to be a more capable hit-to-kill missile interceptor. The SM-3 Block IIA 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.[5] It successfully intercepted a threat-representative ICBM target during a flight test in November 2020.[6] Two Japanese destroyers launched SM-3 Block IIAs (done so for the first time from a Japanese vessel) and successfully made exo-atmospheric intercepts of their targets during a ballistic missile defense test run jointly in Hawaii with the United States in November 2022.[7]

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-2020s) and then foreign satellites.[8] In August 2019, the Japanese MoD released a budget request for FY2020 that included a request for a 4.0 billion yen (USD 38 million) program for a "study on electromagnetic disruption system" and purchasing equipment that could detect when its satellites are being electromagnetically interfered with.[9]

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

2 Ibid.

3 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/.

4 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.

5 Grego, ibid.

6 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/.

7 Dzirhan Mahadzir, "Two Japanese Destroyers Score in Ballistic Missile Defense Test off Hawaii," *USNI News*, November 21, 2022, https://news.usni.org/2022/11/21/two-japanese-destroyers-score-in-ballistic-missile-defense-test-off-hawaii.

8 "Satellite interceptor sought by mid-2020s," ibid.

9 "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.

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 (see Imagery Appendix, pg. 16-58) has a radar facility that can see up to 10 objects of a diameter of 1 meter or greater to an altitude of 2000 km, and the Bisei Space Guard Center (see Imagery Appendix, pg. 16-59) has an optical telescope for SSA tracking to GEO.[10] 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.[11]

In 2019, the United States and Japan announced they were planning to connect their SSA data starting in FY 2023.[12] Japan's SDF does not have its own SSA capabilities but has been working on developing them via US 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 by FY 2022.[13] The Japanese MoD intends for its future SSA network to be composed of both ground- and space-based elements.

In March 2022, the Japanese Air Self-Defence Force (ASDF) announced the creation of a new space operations unit whose mission is SSA; it will operate a satellite that will be launched in FY 2026 and ground-based radar that is still being built in the Yamaguchi prefecture.[14] Additionally, LeoLabs announced in May 2022 it had won a "multimillion" dollar contract to provide SSA data and training to the Japanese ASDF.[15]

The SDF SSA system is intended to be tied to the US SSA network, and both hope to be linked to JAXA's network. The fact sheet for the April 2019 2+2 Dialogue held between US and Japanese officials mentioned the possibility of putting US SSA sensors on Japan's Quasi-Zenith Satellite System (QZSS) GPS augmentation constellation.[16] The USAF's 2021 budget documents included a request for funding two US 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)." [17] In January 2023, the USSF delivered two hosted payloads for SSA that will be integrated into two future QZSS satellites.[18] As of 2022, the Japanese Defense Ministry was actively developing space situational awareness (SSA) laser-detecting capabilities and setting up a second space operations unit that will utilize electromagnetic waves to monitor and discern threats to its satellites.[19]

On March 15, 2023, Northrop Grumman signed a partnership with Japanese company IHI to develop "small, highly maneuverable satellites and other solutions" to aid Japanese SSA capabilities and help protect satellites in GEO.[20]

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 so long as it would be defensive in nature.[21] This was part of a larger shift to thinking about incorporating space into national security needs. The Cabinet office created two organizations 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.[22] 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

10 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.

11 "Japan, US to collaborate on space surveillance," *The Mainichi Japan*, March 30, 2019, https://mainichi.jp/english/articles/20190330/p2a/00m/0na/002000c.

12 Ibid.

13 Ibid.

14 "ASDF space operations unit established to monitor space debris and satellites," The Yomiuri Shimbun, March 19, 2022, https://japannews.yomiuri.co.jp/politics/defense-security/20220319-12551/.

15 Debra Werner, "Japan Air Self Defense Force awards contract to LeoLabs," Space News, May 24, 2022, https://spacenews.com/leolabs-contract-japan-ministry-of-defense/.

16 Joint Statement of the Security Consultative Committee, April 19, 2019, p. 3, https://www.mofa.go.jp/files/000470738.pdf.

17 Theresa Hitchens, "Air Force Funds Hosted Payloads On Japan Sats," *BreakingDefense*, February 19, 2020, https://breakingdefense.com/2020/02/air-force-funds-hosted-payloads-on-japan-sats/.

18 Maddie Saines, "QZSS hosted payloads delivered to Japan," GPS World, January 24, 2023, https://www.gpsworld.com/qzss-hosted-payloads-delivered-to-japan/.

19 "Japan to launch second couterspace operations unit in fiscal 2022," *Nikkei Asia*, November 14, 2021, https://asia.nikkei.com/Politics/Japan-to-launch-second-outer-space-operations-unit-in-fiscal-2022.

20 "Northrop Grumman and IHI sign MOU to work together on small maneuverable satellites," *IHI*, March 15, 2023, https://www.ihi.co.jp/en/all_news/2022/aeroengine_space_defense/1198211_3494.html.

21 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.

22 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/.

mission assurance capability and capability to disrupt opponent's command, control, communications and information."[23] The guidelines also discussed how for space and cyber, "establishing international rules and norms has been a security agenda."[24] 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."[25] 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."[26]

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.[27]

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 US-Japan alliance more "robust" and "to make it a pillar for safeguarding peace and security in both outer space and cyberspace."[28] 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."[29] 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.[30] It was indeed stood up in May 2020 with 20 personnel but is now expected to reach full operations in FY 2023.[31] 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. In December 2022, Japanese officials announced their intention to change the name of the Air Self-Defense Force to the Aerospace Self-Defense Force (ASDF) in order to better represent its interest in strengthening space defense.[32]

In 2021, Japan had a record space budget of nearly $50 billion, up about 23% from the previous year.[33] The Japanese Defense Ministry received a similar budget in 2022. Additionally, the Japanese ASDF and USSPACECOM signed an agreement to increase collaboration on space security. Under the agreement, an ASDF officer will receive an assignment in the US Space Command headquarters at Peterson Space Force Base, Colorado.[34]

In September 2022, Japan formally pledged not to conduct destructive DA-ASAT missile tests, as one of the growing number of signatories to the moratorium on such testing initiated by the United States.[35]

Japan released a new National Security Strategy in December 2022 that would allow it, for the first time, to be able to conduct counterstrike operations using long-range missiles.[36] This move is intended to integrate Japan's air and missile defense systems, and is not intended to be used in its space operations, but does signal a change to Japan's historically defensive posture. The new National Security Strategy also notes that "Japan will drive forward measures to capitalize on Japan's overall space-related capabilities in the field of security, such as strengthening cooperation between the Japan Aerospace Exploration Agency (JAXA) and the SDF."[37] The same month, it was reported that the Japanese cabinet would be working on a de facto space security strategy that is planned to be completed at the earliest in summer 2023.[38]

23 Japanese Ministry of Defense, *National Defense Program Guidelines for FY 2019 and Beyond*, December 18, 2018, p. 20, https://www.cas.go.jp/jp/siryou/pdf/2019boueikeikaku_e.pdf.

24 Guidelines, p. 4.

25 Guidelines, p. 11.

26 Guidelines, p. 12.

27 *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.

28 "Japan To Stand Up Space Domain Mission Unit In April 2020 To Counter Threats To Satellites," *SpaceWatchGlobal*, January 2020, https://spacewatch.global/2020/01/japan-to-stand-up-space-domain-mission-unit-in-april-2020-to-counter-threats-to-satellites/.

29 Mari Yamaguchi, "Abe says new unit will defend Japan from space tech threats," *Associated Press*, January 20, 2020, https://apnews.com/2d88b7c34a5d004eaa59791b8587579d.

30 "Japan to Stand Up," ibid.

31 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.

32 "Japan Plans to Rename Air SDF to "Aerospace" SDF," Nippon.com, December 7, 2022, https://www.nippon.com/en/news/yjj2022120701124/.

33 Park Si-soo, "Japan budgets a record $4.14 billion for space activities," *SpaceNews.com*, March 9, 2021, https://spacenews.com/japan-budgets-a-record-4-14-billion-for-space-activities/; Hana Kusumoto, "Japan seeks record $50 billion defense budget to counter an increasingly aggressive Chain," *Stars and Stripes*, August 31, 2021, https://www.stripes.com/theaters/asia_pacific/2021-08-31/japan-record-defense-budget-f-35-china-2727340.html.

34 Park Si-soo, "Japan to launch 2nd space defense unit to protect satellites from electromagnetic attack," SpaceNews.com, November 15, 2021, https://spacenews.com/japan-to-launch-2nd-space-defense-unit-to-protect-satellites-from-electromagnetic-attack/.

35 "Decision not to conduct Destructive, Direct-Ascent Anti-Satellite Missile Testing," Ministry of Foreign Affairs of Japan, September 13, 2022, https://www.mofa.go.jp/press/release/press3e_000451.html.

36 Jesse Johnson and Gabriel Dominguez, "Japan approves major defense overhaul in dramatic policy shift," Japan Times, December 16, 2022, https://www.japantimes.co.jp/news/2022/12/16/national/japan-dramatic-defense-shift/.

37 National Security Strategy of Japan, Government of Japan, December 2022, https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf.

38 "Japan Eyes Space Security Framework," The Yomiuri Shimbun, December 22, 2022, https://japannews.yomiuri.co.jp/politics/defense-security/20221222-78718/.

At a January 2023 meeting of the US-Japan Security Consultative Committee convened by the US Secretaries of Defense and State and the Japanese Ministers of Defence and Foreign Affairs, the ministers released a statement noting that they considered "attacks to, from, or within space present a clear challenge to the security of the Alliance, and affirmed such attacks, in certain circumstances, could lead to the invocation of Article V of the Japan-US Security Treaty;" invocation of Article V would be made "on a case-by-case basis, and through close consultations between Japan and the United States, as would be the case for any other threat." [39]

In June 2023, Japan released a new Space Security Initiative that outlines the strategy for responding to space threats over the next decade.[40] The document described the changing space security environment and the plan for Japan to increase use of space systems for security on Earth as well as protecting its own use of space. The latter approach focuses on improving the resilience of space systems, more cooperation with allies and between JAXA and the MOD in enhancing SSA, and helping develop international norms of responsible behavior.

Potential Military Utility /

Japan currently possesses 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.

39 Statement released by the Governments of the United States of America and Japan following the U.S.-Japan Security Consultative Committee (SCC) in Washington, D.C., January 11, 2023, https://jp.usembassy.gov/joint-statement-security-consultative-committee-2plus2/.

40 "Space Security Initiative," The Space Development Strategy Headquarters, June 2023, https://www8.cao.go.jp/space/anpo/kaitei_fy05/enganpo_fy05.pdf.

39.0738°N

11

NORTH KOREA

125.8198°E

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 not 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 highly 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 exhibited the capability to jam civilian GPS signals within a limited geographical area. Their capability against 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.

Co-Orbital ASAT Technologies

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

Due to a lack of detected signals and instability of their platforms, both of its two Kwangmyŏngsŏng satellites are thought to have failed soon after launch. 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.[1] However, despite tumbling the satellites were still following a relatively predictable orbital trajectory and have not posed a collision threat to other space objects. Kwangmyŏngsŏng 4 re-entered the atmosphere on June 9, 2023, and Kwangmyŏngsŏng 3-2 re-entered on September 13, 2023.

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. The Malligyong-1 is thought to be able to take at best low-resolution pictures;[2] After the May 2023 launch failure, South Korean officials were able to dredge parts of the satellite and its launch rocket and announced that they assessed that the satellite "has no military utility as a reconnaissance satellite."[3]

There is no indication that North Korea's satellites have 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 Kwangmyŏngsŏng series of satellites conducted maneuvers while in orbit.[4] Any serious attempt at orbital counterspace capabilities would require a sophistication that is beyond North Korea's current technological capacity.

1 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/.

2 "North Korea's spy satellite launch: All you need to know," *Al Jazeera*, November 22, 2023, https://www.aljazeera.com/news/2023/11/22/north-koreas-spy-satellite-launch-all-you-need-to-know.

3 Song Sang-ho, "S. Korea retrieves N. Korean spy satellite wreckage, ends salvage operation: military," *Yonhap News Agency*, July 5, 2023, https://en.yna.co.kr/view/AEN20230705001753325?-section=national/defense.

4 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.

DA-ASAT Technologies

North Korea has multiple ballistic missile 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.[5]

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.[6]

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.[7]

Kim Jong Un announced in the annual 2017 New Year's Address that the country was nearly ready to flight-test an ICBM.[8] There were then two ICBM tests in 2017 of a relatively new system, the Hwasong-14. North Korea tested the Hwasong-14 (KN-20) on July 4, 2017, and July 28, 2017, using a lofted trajectory. Several estimates place the range around 10,000 km, placing US cities and targets in space above LEO potentially at risk.[9] 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 the liquid-fueled ICBM flew on a lofted trajectory to an altitude of 4,500 km.[10] 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." [11] 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 US." [12] There was another launch of an ICBM-class launch vehicle in March 2022; this rocket (either the Hwasong-15 or possibly the newer Hwasong-17) flew a distance of 1100 km and reached an altitude of 6000 km (placing objects in LEO within reach).[13] A Hwasong-17 is suspected to have been launched in November 2022; it failed during its flight test.[14] North Korean officials announced that they had launched a Hwasong-15 in February 2023; it flew a heavily lofted flight and reached a distance of nearly 1000 km at an altitude of about nearly 5800 km.[15] If it had flown a less lofted trajectory, it is thought that it could reach the continental United States, indicating it could likely reach objects in LEO as well.[16] The Hwasong-17, a liquid-fuelled mobile ICBM, was successfully launched in March 2023, at a range of about 1000 km and an altitude of about 6000 km.[17] Three launches of the

5 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/.

6 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.

7 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/.

8 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.

9 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.

10 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/.

11 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.

12 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/.

13 Mike Wall, "North Korea launches most powerful missile yet in 1st ICBM test since 2017: reports," Space.com, March 24, 2022, https://www.space.com/north-korea-launches-most-powerful-icbm-test.

14 Elizabeth Howell, "Launch of North Korea's most powerful ballistic missile fails: reports," Space.com, November 3, 2022, https://www.space.com/north-korea-ballistic-missile-launch-failure-november-2022.

15 Jesse Johnson, "North Korea says surprise ICBM drill is 'proof' of 'nuclear counterattack' capabilities," Japan Times, February 19, 2023, https://www.japantimes.co.jp/news/2023/02/19/asia-pacific/north-korea-icbm-suprise-launch/.

16 Choe Sang-hun, "North Korea Launches ICBM," New York Times, February 18, 2023, https://www.nytimes.com/2023/02/18/world/asia/north-korea-missile-launch.html.

17 Vann H. Van Diepen, "March 16 HS-17 ICBM Launch Highlights Deployment and Political Messages," 38North.org, March 20, 2023, https://www.38north.org/2023/03/march-16-hs-17-icbm-launch-highlights-deployment-and-political-messages/.

Hwasong-18, which is also described as ICBM-class and uses solid propellant, were held in 2023: it had a test flight in April 2023[18]; it flew a second time in July 2023, when it ranged about 1000 km and went to an altitude of about 6000 km[19]; and then flew a third time in December 2023, when it again ranged about 1000 km and went to an altitude of about 6000 km.[20]

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 the second is 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.[21]

North Korea's only known operational space launch vehicle is the Unha-3. It appears to derive design components from the Taepodong-2, which was originally believed by US intelligence to be a possible ICBM.[22] 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 (KMS 3-2, 2012-072A, 39026) in orbit.[23] The Unha-3 was used to put the second satellite, Kwangmyŏngsŏng 4 (KMS 4, 2016-009A, 41332) into orbit in 2016.[24] Commercial imagery in March 2019 of North Korea's Sohae Satellite Launching Station (see Imagery Appendix, pg. 16-24) indicated that it may have returned to normal operations.[25]

FIGURE 11-1 — KWANGMYONGSONG-4

Two views of the purported earth-observation satellite Korea launched in January 2016.
Image credit: chinaspaceflight.com.[26]

The Unha-3 is known to be a multi-stage rocket with liquid propellant requiring a conventional launch pad and extensive visible preparations. The first stage consists of four Nodong engines, making it too large for mobile use.[27]

North Korea's second proven space launch vehicle is the Chollima-1. North Korean news agency KCNA announced in May 2023 that it had tried to use the Chollima-1 to launch its military reconnaissance Malligyong-1 satellite, but failed in the second stage.[28] It was followed up by another attempt in August 2023, with the Chollima-1 again attempting to place the Malligyong-1 in orbit; this time, it failed in its third stage.[29] The third attempt for the Chollima-1 proved to be a success: in November 2023, North Korean officials announced the successful launch of the SLV and the placement of the Malligyong-1 (2023-179A, 58400) into a 512 km by 493 km at 97.43 degrees orbit.[30] North Korea reported that Malligyong-1 was an active remote sensing satellite and had imaged US military bases, but there was debate about its functionality until it maneuvered in a series of steps to raise its perigee in mid February 2024.[31]

18 Soo-Hyang Choi and Josh Smith, "North Korea says test launch was latest Hwasong-18 ICBM," *Reuters*, July 13, 2023, https://www.reuters.com/world/asia-pacific/north-korea-says-it-test-launched-hwasong-18-icbm-wednesday-yonhap-2023-07-12/.

19 Soo-Hyang Choi and Josh Smith, "North Korea says test launch was latest Hwasong-18 ICBM," ibid.

20 Jack Kim, "North Korea says Hwasong-18 ICBM test was response to US hostility," *Reuters*, December 18, 2023, https://www.reuters.com/world/asia-pacific/north-korea-says-it-conducted-hwasong-18-icbm-monday-yonhap-2023-12-18/.

21 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/; Gunter D. Krebs,"Hwasong-13 ("KN-08", "KN-14") IRBM," Gunter's Space Page, retrieved February 26, 2023, https://space.skyrocket.de/doc_lau/hwasong-13.htm.

22 John Schilling, "Where's That North Korean ICBM Everyone Was Talking About?" *38 North*, March 12, 2015, https://www.38north.org/2015/03/jschilling031215/.

23 Center for Strategic and International Studies, "Taepodong-2 (Unha-3)," https://missilethreat.csis.org/missile/taepodong-2/.

24 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.

25 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/.

26 "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.

27 Center for Strategic and International Studies, "Taepodong-2 (Unha-3)," https://missilethreat.csis.org/missile/taepodong-2/.

28 Song Sang-ho and Chae Yun-hwan, "N. Korea's attempt to launch 1st spy satellite fails after 'abnormal' flight: S. Korean military," *Yonhap News Agency*, May 31, 2023, https://m-en.yna.co.kr/view/AEN20230418005560325?section=nk/nk.

29 Park Si-soo, "North Korea's spy satellite launch fails again," *SpaceNews*, August 24, 2023, https://spacenews.com/north-koreas-spy-satellite-launch-fails-again/.

30 Stephen Clark, "North Korea launched a satellite, then apparently blew up its booster," Ars Technica, November 22, 2023, https://arstechnica.com/space/2023/11/north-korea-launched-a-satellite-then-apparently-blew-up-its-booster/.

31 Marco Langbroek, "A perigee-raising maneuvre by the North Korean satellite Malligyong-1," SatTrackCam Leiden (b)log, February 27, 2024, https://sattrackcam.blogspot.com/2024/02/a-perigee-raising-manoeuvre-by-north.html.

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 US 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.[32] Additionally, it is unknown how large of a yield from a nuclear warhead is necessary to affect the US electrical grid.[33] Although North Korea likely demonstrated a thermonuclear capability in September 2017,[34] 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 in space, such as the US Starfish Prime test in 1962, are known to have generated effects that damaged or destroyed satellites in orbit at the time.[35] However, it would be difficult to predict the ability of creating such effects against military satellites, particularly since many US military satellites are hardened against radiation and EMP effects.

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.[36] This type of interference (downlink jamming) targets GPS receivers within range of the source of the jamming signal but has no impact on the GPS satellites themselves nor the service provided to users outside the range of the jammers. The area affected will depend on the power emitted by the jammer and the local topography. In the case of the reported North Korean incidents, the range was estimated to be several tens of kilometers.

According to unnamed US officials, this type of jamming would not affect US military members who use the military GPS signals.[37] 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 - US 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 extremely limited public information about whether North Korea could 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.[38] However, there is only one report from 2012 about North Korea possibly jamming military communications being broadcast from a South Korean satellite.[39] It is assessed that uplink jamming of communication satellites has otherwise not or has 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 publicly-available information available on this subject.

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.[40] 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).[41] North Korea has been reported to have Iranian phased array radars as part of its air defense network; their capabilities are unknown.[42]

32 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/.

33 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/.

34 *North Korea: Overview*, Nuclear Threat Initiative, last updated October 2020, https://www.nti.org/learn/countries/north-korea/.

35 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.

35 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.

36 "North Korea 'jamming GPS signals' near South border," *BBC News*, April 1, 2016, http://www.bbc.com/news/world-asia-35940542.

37 "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.

38 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/.

39 Martyn Williams, "Report: DPRK Jams South Korean Satellite Comms," North Korea Tech, November 17, 2012, https://www. northkoreatech.org/2012/11/17/report-dprk-jams-south-korean-satellite-comms/.

40 Joseph S. Bermudez Jr., "NADA General Satellite Control Building," *38North.org*, March 22, 2018, https://www.38north.org/2018/03/nada032318/.

41 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/.

42 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.

Counterspace Policy, Doctrine, and Organization

To date, there is no clear doctrine for counterspace weapons in the DPRK. Furthermore, there is an 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.[43] 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 and to use science and technology to solve scientific and technological problems essential to economic construction and people's lives."[44] In November 2021, the North Korean aerospace sector facilitated a space conference to discuss peaceful space development plans and linking satellite technology to economic growth. The conference occurred after Kim Jong Un ordered the development of military reconnaissance satellites earlier in 2021, demonstrating a potential increase in desire to develop space assets and technology.[45] North Korean leader Kim Jong Un visited Sohae in March 2022 and called for it to be "modernized" so to "enable large carrier rockets to be launched there,"[46] which indicates that SLV capabilities continue to be an increased priority for the North Korean government. Satellite imagery taken later in 2022 indicate that construction is in full swing at Sohae, presumably to carry out the modernization called for by Kim.[47]

Potential Military Utility /

North Korea likely possesses very limited military counterspace capabilities. It lacks significant SSA capabilities, demonstrated hit-to-kill capabilities, or any sort of RPO capabilities, and has very limited space launch capabilities. This very likely limits North Korean counterspace options to broad area attacks such as nuclear detonations 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 and would likely engender intense international outrage.

43 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.

44 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.

45 Colin Zwirko, "North Korea holds space conference, says launching satellites will help economy," NK News, November 22, 2021, https://www.nknews.org/2021/11/north-korea-holds-space-conference-says-launching-satellites-will-help-economy/.

46 "N.Korea calls for satellite site 'expansion' as US slams ICBM tests," Agence France-Presse, March 11, 2022, https://www.spacewar.com/reports/NKorea_calls_for_satellite_site_expansion_as_US_slams_ICBM_tests_999.html.

47 Peter Makowsky, Jack Liu, and Jenny Town, "Sohae Satellite Launch Station: Site Upgrades Begin in Earnest," 38North.org, September 6, 2022, https://www.38north.org/2022/09/sohae-satellite-launch-station-site-upgrades-begin-in-earnest/.

37.5665°N

12

SOUTH KOREA

126.9780°E

Assessment /

Over the last several years, South Korea has had a growing focus on military space capabilities. It is working to enhance the space capabilities of its Air Force through the establishment of a Space Operations Center, cooperating with the United States on sharing SSA capabilities, and developing its own longer-range ballistic missiles and space launch vehicles; it also has expressed interest in developing its own reversible counterspace capabilities.

Specifics /

DA-ASAT Technologies

There is no public evidence that South Korea has developed, or is developing, a dedicated DA-ASAT capability. However, it does have a significant ballistic missile program, and is putting an extensive amount of resources into developing its indigenous space launch program, which could theoretically be used as part of a future DA-ASAT capability. It would still need to be combined with several other technologies that South Korea has not yet tested either, such as HTK intercepts.

In October 2021, South Korea launched its first domestically built rocket ("Nuri") with a dummy satellite (which failed to make it to orbit); Nuri is estimated to have cost $1.6 billion to develop.[1] The three-stage liquid-fueled rocket was built by the Korea Aerospace Research Institute (KARI), the civilian space agency in South Korea.[2] President Moon Jae-in said, "We will use our launch vehicles to achieve the dream of landing on the moon by 2030."[3] A June 2022 launch of the Nuri SLV was reported to have put six satellites into orbit, marking the first time an indigenously built South Korean launch vehicle was able to do so.[4] A fire broke out at the Naro Space Center in January 2023 while researchers were working on a follow-on SLV for the Nuri, known as KSLV-III, a launch vehicle which is intended to be launched three times by 2032.[5]

In March 2022, South Korean officials announced the successful launch of a "solid-fueled space projectile" which tested separating a dummy satellite from the launch vehicle as part of a test run by Agency for Defense Development (ADD).[6] A second test of the solid-fueled launch vehicle was successfully flown in December 2022, and was justified by the South Korean Ministry of Defense as, "The South Korean military will greatly develop its own space-based surveillance and reconnaissance capabilities based on the technology and know-how associated with solid propulsion engines."[7]

The inaugural flight of the Nuri finally occurred on May 25, 2023, and successfully placed 8 satellites in LEO.[8]

Additionally, South Korea's military technology agency, the Korea Research Institute for Defense Technology Planning and Advancement (KRIT), released a report "Defense Science & Technology Level Assessment by Country" in January 2022 that argued the country needed "strategic" and "intensive" investments in space weapons in order to keep up with other military powers.[9] According to KRIT, "The space weapon system is the field that requires intensive research and development, considering the conditions of the future battlespace and South Korea's possession of some projectile technologies including the test-launch of Nuri… But as South Korea is far behind the US in the technology, we view that strategic investment is needed." It is unclear what sort of space weapons the report is calling for more R&D on.

1 "South Korea launches first homegrown space rocket Nuri," *BBC News*, October 21, 2021, https://www.bbc.com/news/world-asia-58990718.

2 "South Korea tests 1st domestically made rocket as it pursues satellite launch program," *Associated Press*, October 21, 2021, https://www.npr.org/2021/10/21/1047901483/south-korea-tests-1st-domestically-made-rocket-as-it-pursues-satellite-launch-pr.

3 Yosuke Onchi, "South Korea chases global ambitions in space and defense," *Nikkei Asia,* November 7, 2021, https://asia.nikkei.com/Business/Aerospace-Defense/South-Korea-chases-global-ambitions-in-space-and-defense.

4 Mike Wall, "South Korea's homegrown Nuri rocket launches satellites into orbit for 1st time," Space.com, June 22, 2022, https://www.space.com/south-korea-nuri-rocket-launch-success.

5 "Fire breaks out at space center during fuel test for next generation space rocket," Yonhap News Agency, February 1, 2023, https://en.yna.co.kr/view/AEN20230201009700320.

6 Jeongmin Kim, "South Korea tests indigenous solid-fuel rocket week after North's ICBM launch," NK News, March 30, 2022, https://www.nknews.org/2022/03/south-korea-tests-indigenous-solid-fuel-rocket-week-after-norths-icbm-launch/?t=1656492835423.

7 Jeongmin Kim, "Seoul boasts of space vehicle launch as it looks to better surveil North Korea," NK News, January 2, 2023, https://www.nknews.org/2023/01/seoul-boasts-of-space-vehicle-launch-as-it-looks-to-better-surveil-north-korea/.

8 Hyung-Jin Kim, "South Korea launches first commercial-grade satellite, as North Korea plans first spy satellite," *Associated Press*, May 25, 2023, https://apnews.com/article/south-korea-satellite-launch-dafad1ed70da24e549bcfafe19ec7654.

9 Ji Da-gyum, "S.Korea ranks 9th in defense tech, but needs 'intensive' R&D in space weapons," The Korea Herald, January 10, 2022, http://www.koreaherald.com/view.php?ud=20220110000713.

Electronic Warfare

As part of its Space Odyssey 2050 program, the South Korean Air Force is working on EW counterspace capabilities that can be used to deter or counter adversary space capabilities.[10] Few public details are known about the state of development or planned capabilities for this system.

Space Situational Awareness

As part of an August 2021 agreement between the ROK and US militaries, the two countries will hold joint drills to improve SSA. The ROK is working to enhance its indigenous SSA capabilities through developing its own SSA infrastructure that can be operational by the mid-2020s.[11] It is anticipated to include a space weather forecast system, reconnaissance satellites, and an electro-optical satellite surveillance system. In August 2021, military officials from South Korea and the United States agreed to cooperate on security space issues. Signed between Gen. Park In-ho, ROK Air Force chief of staff, and General Raymond, USSF chief of space operations, this agreement established a joint consultative body on space policy.[12] They also agreed to share information on SSA and work to enhance joint space operations capabilities.[13] ROK Air Force Colonel Park Ki-tae, chief of the Space Operations Center, indicated SSA is a priority for the South Korean Air Force, stating in October 2021 that "What we urgently need is 'eyes' to look at what's happening in outer space."[14] The bilateral Space Cooperation Working Group that met in Washington, DC, in April 2022 resulted in another signed agreement on cooperation on space security issues, including sharing SSA data, and the creation of a joint space policy research organization.[15]

Counterspace Policy, Doctrine, and Organization

In 2013, the South Korean Air Force unveiled its "Space Odyssey 2050", a three-part strategy that aims to build its own space capabilities by 2050 to protect South Korea's military forces. As part of the strategy, the South Korean Air Force plans to develop the ability to monitor and "counter" space threats.[16]

The ROK Air Force launched its Space Operations Center in September 2021, which is charged with creating and carrying out space policy, as well as working with other branches of the South Korean government on enhancing space capabilities.[17] It will have three departments: one for sharing space information, one for space policy development, and one for developing space weapons. According to Air Force Chief of Staff Gen. Park In-ho, "The Air Force's space center will focus its capabilities on developing our national defense space force through building space weaponry, training professionals, and strengthening the organization. That will strengthen our national security in space and enable the Air Force to become a space force."[18]

South Korean officials announced that they intended to spend $619 million on space programs in 2022, a 15% increase from 2021 levels; of this, $175.8 million was slated for SLV development.[19] $70 million was intended to be spent on developing the Korea Positioning System, South Korea's planned PNT constellation of eight satellites to be deployed between 2027 and 2034.

In October 2022, South Korea formally pledged not to conduct destructive DA-ASAT missile tests, as one of the growing number of signatories to the moratorium on such testing initiated by the United States.[20]

10 "Air Force Sets up Space Center," KBS News, September 30, 2021, https://world.kbs.co.kr/service/news_view.htm?lang=e&Seq_Code=164568.

11 Park Si-soo, "US-South Korea joint space drills to focus on space situational awareness," *Space News*, October 27, 2021, https://spacenews.com/us-south-korea-joint-space-drills-to-focus-on-space-situational-awareness/.

12 Park Si-soo, "US, South Korea agree to enhance security cooperation in outer space," *SpaceNews*, August 30, 2021, https://spacenews.com/us-south-korea-agree-to-enhance-security-cooperation-in-outer-space/.

13 Park, August 30, 2021, ibid.

14 Park, October 27, 2021, ibid.

15 "ROK, US defense ministries hold 18th ROK-US Space Cooperation Working Group," Office of the President, Republic of Korea, May 16, 2022, https://eng.president.go.kr/briefing/ZrBC4wVq; Park Si-soo, "U.S., South Korea agree to cooperate on space situational awareness for military purposes," *SpaceNews*, April 26, 2022, https://spacenews.com/u-s-south-korea-agree-to-cooperate-on-space-situational-awareness-for-military-purposes/.

16 "Air Force Sets up Space Center," *KBS News*, September 30, 2021, https://world.kbs.co.kr/service/news_view.htm?lang=e&Seq_Code=164568.

17 "Air Force Sets up Space Center," *KBS World*, September 30, 2021, https://world.kbs.co.kr/service/news_view.htm?lang=e&Seq_Code=164568.

18 Kwon Hyuk-chul, "S. Korean Air Force opens space center to bolster space strategy," *Hankyoreh*, October 1, 2021, https://english.hani.co.kr/arti/english_edition/e_national/1013584.html.

19 Park Si-soo, "South Korea's double-digit space budget boost," Space News, April 21, 2022, https://spacenews.com/south-koreas-double-digit-space-budget-boost/.

20 Statement by H.E Joonkook Hwang, Permanent Representative of the Republic of Korea to the United Nations First Committee of the 77th Session of the General Assembly / General Debate New York, October 4, 2022, https://overseas.mofa.go.kr/un-en/brd/m_24404/view.do?seq=11&page=2.

In March 2023, South Korea announced another significant increase in spending on space programs of $674 million, an increase of 19.5% from 2022.[21] The second biggest item in the budget ($113.6 million) is for development of a next-generation space launch vehicle, and the third biggest item ($73.1 million) is for space defense programs.

In April 2023, South Korea announced plans to hold a table-top exercise with military and government officials to examine how to respond to dangers from space and strengthen coordination between the military and space-related agencies.[22]

Potential Military Utility

In theory, South Korea's indigenously-developed space launch and ballistic missile expertise could be leveraged for a future DA-ASAT capability. However, given that South Korea has not tested additional technologies, such as hit-to-kill intercept, it is unlikely to be very capable. Also, since South Korea does not have an indigenous SSA capability yet, its ability to target objects in orbit is questionable; however, it does intend to develop its SSA capabilities within the middle of the decade and it has signed an SSA-sharing agreement with the United States, it is possible that this could change. The South Korean Air Force may have a basic EW counterspace capability through its Space Odyssey 2050 program, although again this is in very early stages (if it does indeed exist anywhere outside a planning document).

21 Park Si-soo, "South Korea sets record space budget to bolster industry, develop new rocket," *SpaceNews*, March 31, 2023, https://spacenews.com/south-korea-sets-record-space-budget-to-bolster-industry-develop-new-rocket/.

22 Chae Yun-hwan, "S. Korea to hold tabletop exercise against space hazards," *Yonhap*, April 12, 2023, https://en.yna.co.kr/view/AEN20230412003300325.

51.5072°N

13

THE UNITED KINGDOM

0.1276°W

Assessment /

The United Kingdom has long played a supporting role in military space activities through its participation in NATO and its bilateral relationship with the United States. Over the past few years, the United Kingdom has begun to add additional elements to increase its indigenous military space capabilities, primarily in SSA and policy, organization, and doctrine. To date, the United Kingdom has not publicly announced any specific plans to develop offensive counterspace capabilities.

Specifics /

Space Situational Awareness

RAF Fylingdales (see Imagery Appendix, pg. 16-32) has been the site of an operational radar since 1963, providing ballistic missile early warning to the US and UK governments.[1] Furthermore, as part of its participation in the Space Surveillance Network, its solid-state phased array radar can track objects to an altitude of 3000 nautical miles.[2] UK space surveillance technology is being incorporated into the European Space Agency (ESA)'s first coordinated tracking campaign by contributing, via the UK Space Agency (UKSA), the capabilities of the Chilbolton Observatory (a meteorological radar experimental facility) and Space Insight's Starbrook (an optical space surveillance sensor system).[3] The Chilbolton Advanced Meteorological Radar (CAMRa) can detect objects with a radar cross section as small as 1 square meter as far as 1000 km in altitude, while the Starbrook sensor can detect objects down to 1 meter as far as 40,000 km in altitude.[4] In April 2023, the United Kingdom asked industry to propose bids for a new ground-based telescope located at a UK military base in Cyprus.[5]

The United Kingdom and the United States signed an SSA data sharing agreement in September 2014.[6]

In early 2022, the UKSA announced a pilot program called "Monitor Your Satellites," a service where operators of UK-based satellites could get warnings of close approaches between their satellites and other space objects.[7] While it was invite-only at the beginning, it was eventually opened up to all UK operators and by October 2022, one-third of all UK satellite operators had signed up for the service.[8]

In June 2023, the United Kingdom created a Joint Task Force Space-Defense Commercial Operations Cell (JCO) to augment the existing US JCO located at Schriever Space Force Base in Colorado.[9] The UK SCO will be integrated with the US JCO to enable operators to more easily track space objects around the clock.

In December 2023, the United States announced that Australia and the United Kingdom had officially joined the Deep Space Advanced Radar Capability (DARC) program.[10] DARC is an effort to develop a new set of radars to detect, track, and identify objects in deep space and consists of three geographically distributed sites that each have multiple transmit and receive radars meshed together (see US Space Situational Awareness Capabilities, Section 1.5).

Counterspace Policy, Doctrine, and Organization

The United Kingdom participates in the US-led Combined Space Operations Center; other participants include Australia, Canada, France, Germany, New Zealand, Italy, Norway, and Japan.

The UK Space Command was formed in April 2021 (at RAF High Wycombe, where the RAF Air Command is located as well) with the goal of providing

1 *RAF Fylingdales: The Station*, Royal Air Force, accessed February 21, 2022, https://www.raf.mod.uk/our-organisation/stations/raf-fylingdales/.

2 "RAF Fylingdales," *Wikipedia*, last edited February 6, 2022, https://en.wikipedia.org/wiki/RAF_Fylingdales#Systems.

3 "UK technology scans the skies for space hazards," RAL Space, accessed February 26, 2023, https://www.ralspace.stfc.ac.uk/Pages/UK-technology-scans-the-skies-for-space-hazards.aspx.

4 "UK technology scans the skies for space hazards," ibid.

5 Tim Martin, "UK asks industry for new ground-based space domain awareness sensor capability for Cyprus base," *BreakingDefense*, April 20, 2023, https://breakingdefense.com/2023/04/uk-asks-industry-for-new-ground-based-space-domain-awareness-sensor-capability-for-cyprus-base/.

6 "DOD Signs Space Data Sharing Agreement with UK," *U.S. Strategic Command Public Affairs*, September 25, 2014, https://www.stratcom.mil/Media/News/News-Article-View/Article/983787/dod-signs-space-data-sharing-agreement-with-uk/.

7 "Case Study: Monitor Your Satellites," UK Space Agency, May 10, 2022, https://www.gov.uk/government/case-studies/monitor-your-satellites.

8 "How satellite operators are shaping a new collision assessment service," UK Space Agency Blog, October 18, 2022, https://space.blog.gov.uk/2022/10/18/how-satellite-operators-are-shaping-a-new-collision-assessment-service/.

9 Theresa Hitchens, "New UK military 'cell' to partner with US SPACECOM on space domain awareness," *BreakingDefense*, June 26, 2023, https://breakingdefense.com/2023/06/new-uk-military-cell-to-partner-with-us-spacecom-on-space-domain-awareness/.

10 "US, UK, Australia annouce trilateral Deep Space Advanced Radar Capability Initiative," United States Space Force, December 2, 2023, https://www.spaceforce.mil/News/Article-Display/Article/3604036/us-uk-australia-announce-trilateral-deep-space-advanced-radar-capability-initia/.

command and control of all the United Kingdom's space capabilities; oversight of the development of space-based capabilities; strengthen space workforce development; and continue the United Kingdom's participation in the Combined Space Operations initiative.[11] It is operated jointly by the RAF, Royal Navy, and the Army.

The United Kingdom released its national space strategy (NSS) in September 2021.[12] In it, the United Kingdom identified its national vision for space, which included "the UK will grow as a space nation" and "We will protect and defend UK interests in space."[13] It had five goals for the United Kingdom in space; number four was "Protect and defend our national interests in and through space," mostly through resiliency, collaboration, and integration.[14] It also highlighted the need for diplomacy, stating, "The UK will deliver global leadership on a safe, sustainable, and secure space environment working through international and intergovernmental forums and with our partners and allies."[15] Specifically relevant to this document, the NSS also said, "We will support global stability through arms control and non-proliferation regimes and will work with allies to deter hostile activity against space systems including the use of weapons in space."[16]

The United Kingdom released its defence space strategy (DSS) in February 2022. In it, the United Kingdom noted the need "to both protect and defend the UK's equities in space and the services derived from space assets."[17] UK Space Command is tasked with leading the country's approach to space. Investments in SDA, space control, and command and control are prioritized; a joint military-civilian National Space Operations Centre will be created through the enhancement of the UKSpOC (UK Space Operations Centre) and cooperation with the UKSA.[18] The "own, collaborate, or access" framework was used to define how the United Kingdom will work to achieve space capabilities.[19] It should be noted that space was described as the UK's fifth operational domain, not a warfighting domain. China and Russia were identified as examples of international threats to space.[20] One of the strategic themes was to protect and defend; it called out SDA as a way in which the United Kingdom "will improve our ability to generate appropriate measures to protect and defend our critical space capabilities. This suite of integrated, high-tech capabilities that can collect, process, exploit and transmit data, information, and intelligence activity in space."[21] It also stated that the United Kingdom will work "to enhance space diplomacy, leveraging existing alliances and partnerships to establish norms of behaviour for the space domain."[22] Finally, in discussing space control, it stated that "we will invest over £145M in additional funding over the next 10 years. We will investigate mechanisms to deliver carefully calibrated effects to assure our access to, and operational independence in, space."[23]

As part of its new military space strategy, the United Kingdom intends to invest $1.9 billion in military space satellite capabilities.[24] Most of it is dedicated to the Istari program, which is planned to provide military ISR and laser communications capabilities; as well, it has the Minerva program, which is intended to create a satellite network in support of military operations that can take in information and process it from UK and ally satellites. According to Jeremy Quin, Minister for Defense Procurement, these two satellite networks will be "building blocks" of the United Kingdom's future military space architecture.[25]

The United Kingdom released its keystone military doctrine publication on space, Space Power, in September 2022.[26] It is intended to "provide a basis for understanding the utility of the space domain in the military context,"[27] and identifies four key space power roles: space domain awareness, space control, space support to operations, and space service support.[28] Space control is

11 *Guidance: UK Space Command*, UK Ministry of Defence, April 1, 2021, https://www.gov.uk/guidance/uk-space-command.

12 National Space Strategy, HM Government, September 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1034313/national-space-strategy.pdf.

13 National Space Strategy, ibid, p. 6.

14 National Space Strategy, ibid, p. 20.

15 National Space Strategy, ibid, p. 33.

16 National Space Strategy, ibid, p. 34.

17 Defence Space Strategy: Operationalising the Space Domain, UK Ministry of Defence, February 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1051456/20220120-UK_Defence_Space_Strategy_Feb_22.pdf, p. 6.

18 Defence Space Strategy, ibid, p. 7.

19 Defence Space Strategy, ibid.

20 Defence Space Strategy, ibid, p. 11-12.

21 Defence Space Strategy, ibid, p. 19.

22 Defence Space Strategy, ibid, p. 20.

23 Defence Space Strategy, ibid, p. 32.

24 Sandra Erwin, "U.K. announces $2 billion in new funding for military space programs," *Space News*, February 1, 2022, https://spacenews.com/u-k-announces-2-billion-in-new-funding-for-military-space-programs/.

25 Erwin, "U.K. announces," ibid.

26 Joint Doctrine Publication (JDP) 0-40, *UK Space Power*,' UK Ministry of Defence, September 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1111805/JDP_0_40_UK_Space_Power_web.pdf.

27 JDP 0-40, ibid, p. v.

28 JDP 0-40, ibid, p. 29.

defined as "the use of defensive and offensive capabilities to assure access and freedom of action in space."[29] While the overall document is written to follow what it calls a "NATO-first approach" (for example, it calls space one of five interconnected "operational domains"), it notes that, "given the close ties with United States Space Forces, it is also coherent with current United States space doctrine."[30]The doctrine notes that "deterrence in, through or using space capabilities is not an independent activity but must form part of the wider strategy. It is a whole-of-government activity to which Defence contributes," and emphasizes that UK deterrence posture "remains enshrined in NATO" through article 5 of the NATO treaty.[31]

In October 2022, the United Kingdom formally pledged not to conduct destructive DA-ASAT missile tests, as one of the growing number of signatories to the moratorium on such testing initiated by the United States.[32]

Potential Military Utility

Although it possesses some of the underlying technologies, such as indigenous ballistic missile expertise, the UK is very unlikely to develop DA-ASAT capabilities. It has not expressed any interest in doing so and has not developed policies allowing it as an option (its military space doctrine focuses largely on SSA capabilities). It does not have an indigenous space launch capacity. The UK has also not shown an interest in or the technological capability for a future co-orbital ASAT program. Based on the UK's solid existing SSA capabilities and the evolution thereof (in terms of offering conjunction warnings to UK satellite operators), it is possible that its SSA capabilities could provide some military utility for both offensive and defensive counterspace operations.

29 JDP 0-40, ibid, p. 34.

30 JDP 0-40, ibid, p. v.

31 JDP 0-40, ibid, p. 80.

32 "Responsible space behaviours: the UK commits not to destructively test direct ascent anti-satellite missiles," press release from the Foreign, Commonwealth & Development Office and UK Space Agency, October 3, 2022, https://www.gov.uk/government/news/responsible-space-behaviours-the-uk-commits-not-to-destructively-test-direct-ascent-anti-satellite-missiles.

Cyber Counterspace Capabilities

3

14

GLOBAL CYBER COUNTER-SPACE CAPABILI-TIES

Assessment /
Multiple countries likely possess cyber capabilities that could be used against space systems; however actual evidence of cyber attacks in the public domain is limited. The United States, Russia, China, France, 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, and nearly all have gone after the end user segment and not satellites themselves.

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 destructive and non-destructive. 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 the 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.[1]

Some bugs can lead to vulnerabilities, which are weaknesses in a computer system that can be leveraged by an attacker to breach a system. An exploit is an active attack that takes advantage of a specific vulnerability.

Any cyber attack requires four things: access, vulnerability, a malicious payload, and a command-and-control system.[2] Three primary points of access exist for exploitation, attack, and service denial of space assets in the cyber domain: the supply chain, the extended land-based infrastructure that sustains space-based assets—including ground stations, terminals, related companies, and end-users—and the satellites themselves.[3] Successful penetration of any one of these may be sufficient to produce the desired espionage, ‘soft’-,

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

2 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/.

3 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*, September 2016, 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.

or 'hard'-kill effects, and also enables the launching of additional follow-on cyberattacks in other vectors.[4] 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.[5] 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.[6] In 2017, the US 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 US military advantages, are certain to continue to pursue a "full range" of counter-space capabilities.[7] 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.[8]

4 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/cyber-security-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.

5 "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/cyber-attacks-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.

6 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.

7 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.

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

Categories of Cyber Attacks on Space Systems

Parsing the exact nature and extent of cyber capabilities or development efforts with any precision based on open sources 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. Cyber weapon development is also 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.

The first category of cyber attacks against space systems are deliberate installation of hidden back doors in hardware or software products, which are made possible by flaws in global supply chain security.[9] Such back doors have been found in Chinese electronics [10] and Russian software packages [11] used by US 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.[12] There have also been media reports of US intelligence agencies intercepting shipments of commercial equipment to install "implants" [13], and creating backdoors in commercial encryption software.[14] 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 against space systems 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.

9 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.

10 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.

11 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 Journa*l, October 5, 2017, https://www.wsj.com/articles/russian-hackers-stole-nsa-data-on-u-s-cyber-defense-1507222108.

12 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.

13 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/.

14 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 US commercial satellite.[15] 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 US-China Economic and Security Review Commission.[16] In October 2007, the Landsat 7 (1999-020A, 25682) remote sensing satellite experienced twelve minutes of interference. In June 2008, the Terra (1999-068A, 25994) 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 7 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.[17] General Robert Kehler, then commander of United States Strategic Command, said there was no evidence to attribute the attacks at the time.[18]

The third category of cyber attacks against space systems involves attacks on terrestrial C2 or data relay stations. Techniques could include fly-overs with manned aircraft, unmanned aerial systems (UAS), or weather balloons;[19] 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; [20] physical access, through either covert infiltration or social engineering; [21] and network exploitation or attack, using traditional means.[22] 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).[23] 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.[24]

15 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.

16 "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.

17 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.

18 Ibid.

19 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/.

20 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/.

21 Ibid.

22 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.

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

24 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 spatial data. NASA, for example, has long been the target of cyberattacks, as have other space agencies around the world.[25] In 2011, attackers gained full access to 18 servers supporting multiple missions at the Jet Propulsion Laboratory and stole 87 gigabytes of data.[26] 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).[27] 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 US government did not publicly attribute the attack, US Rep. Frank Wolf declared that "NOAA told me it was a hack and it was China." [28] 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.[29] In a similar fashion, attackers from the hacker collective Anonymous reportedly breached the website of the Russian Space Research Institute (IKI) in March 2022 in response to the invasion of Ukraine.[30]

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 US university students developed a technique for attacking the software in common commercial GPS receivers.[31] The attack uses a specially built box that modifies the data content of real civil GPS signals and rebroadcasts 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.[32]

25 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.

26 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.

27 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.

28 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.

29 Security Response Attack Investigation

30 Joseph Cox, "Hackers Breach Russian Space Research Institute Website," Vice, March 3, 2022, https://www.vice.com/en/article/z3n8ea/hackers-breach-russian-space-research-institute-website.

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.

31 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.

32 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, https://ieeexplore.ieee.org/document/6142258; 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.

Case Study: Case Study: Cyber Attacks Against Multiple Satellite Networks During The Russian-Ukrainian War

Several concrete examples of cyber attacks against the user segment of a space system have occurred as part of the ongoing Russian invasion of Ukraine. Within hours of Russian troops crossing the border into Ukraine in February 2022, tens of thousands of end user modems for the KA-SAT satellite communications service, managed by the US-based company Viasat, went offline.[33] The affected users included thousands of wind turbines in Germany and many other individuals and businesses across Europe, including the Ukrainian government and police, and other networks that resold the KA-SAT service in France, Hungary, Greece, Italy, and Poland.[35] Subsequent details from Viasat revealed that the attack began with a denial-of-service attack within Visat's customer network that appeared to emanate from equipment located within Ukraine. This was followed by tens of thousands of customer modems disconnecting from the network. Further analysis discovered an external attacker used a misconfigured VPN appliance to gain access to the management network for the KA-SAT service and sent a series of malicious commands to overwrite data on user modems. Although Viasat originally claimed the modems were not permanently damaged, analysis done by the cyber security firm SentinelOne discovered a new type of destructive wiper malware called AcidRain was used in the attack, a claim later confirmed by Viasat.[36]

On May 10, 2022, the United States, United Kingdom, and European Union publicly attributed the cyber attack against Viasat's KA-SAT services to Russia, and specifically to hackers working for the Main Directorate of the General Staff of the Armed Forces of the Russian Federation, commonly known as the GRU.[37] US Secretary of State Anthony Blinken stated that there were strong similarities between the AcidRain wiper malware and other wiper malware used by Russian military cyber operators as part of the armed conflict in Ukraine.[38]

Independent analysts suggested that the aim of the cyber attack was to cripple Ukrainian communications, noting that the attack occurred one hour before the first Russian troops crossed the border, although evidence of the attack's actual impact on the war remains under debate.[39]

Shortly after the attack, Ukrainian officials publicly called on SpaceX CEO Elon Musk to provide Ukraine terminals for the Starlink broadband communications system, which he did by the thousands. Ukraine was able to use Starlink to replace many links in its civilian and government communications system, and even used the service to directly support military operations against Russia. In November 2022, a pro-Russian hacktivist group known as Killnet claimed to have launched a distributed denial-of service attack against Starlink, and some users reported difficulty logging in for a brief time.[40] However, Musk has since stated that SpaceX had "reprioritized to cyber defense and overcoming signal jamming" and as of February 2024, the Starlink service appears to have been remarkably resistant to further cyber attacks.[41]

In June 2023, it was reported that a cyber attack was directed at Dozor-Teleport, a Russian satellite communications provider used by the military and security services. Both the mercenary group PMC Wagner and a hacktivist collective claimed responsibility for the attack, which reportedly damaged ground control infrastructure, including user terminals, and resulted in the service being offline for 14 hours.[42]

Taken together, these three incidents indicate that cyber attacks on space

33 Matt Burgess, "A mysterious satellite hack has victims far beyond Ukraine," Arstechnica, March 24, 2022, https://arstechnica.com/information-technology/2022/03/a-mysterious-satellite-hack-has-victims-far-beyond-ukraine/.

34 "'Cyberattack' knocks thousands offline in Europe," Insider Paper, March 4, 2022, https://insiderpaper.com/cyberattack-knocks-thousands-offline-in-europe/.

35 "KA-SAT Network cyber attack overview," Viasat, March 30, 2022, https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.

36 Juan Andres-Guerrero-Saade, "AcidRain: A Modem Wiper Rains Down on Europe," SentinelLabs, March 31, 2022, https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/.

37 Dan Goodin, "US and its allies say Russia waged cyberattack that took out satellite network," Arstechnica, May 10, 2022. https://arstechnica.com/information-technology/2022/05/us-and-its-allies-say-russia-waged-cyberattack-that-took-out-satellite-network/.

38 Anthony J. Blinken, "Attribute of Russia's Malicious Cyber Activity Against Ukraine," U.S. Department of State, May 10, 2022, https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/.

39 Jon Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications," Carnegie Endowment for International Peace, December 16, 2022, https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657.

40 Becky Bracken, "Killnet gloats about DDoS attacks downing Starlink, White House," Dark Reading, November 29, 2022, https://www.darkreading.com/threat-intelligence/killnet-gloats-ddos-attacks-starlink-whitehouse-gov.

41 Jeff Foust and Brian Berger, "SpaceX shifts resources to cybersecurity to address Starlink jamming," *SpaceNews*, March 5, 2022, https://spacenews.com/spacex-shifts-resources-to-cybersecurity-to-address-starlink-jamming/.

42 Joseph Menn, "Cyberattack knocks out satellite communications for the Russian military," The Washington Post, June 30, 2023, https://www.washingtonpost.com/technology/2023/06/30/satellite-hacked-russian-military/.

systems are likely to occur as part of future armed conflicts which incorporate more military and commercial space systems.

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".[43] 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.[44] 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.[45] 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.[46]

In 2014, Crowdstrike released a report tracking 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."[47] Dubbed "Putter Panda," the group was found to have conducted comprehensive and sustained penetration and cyber-espionage operations targeted at the US defense and European satellite and aerospace industries since at least 2007.[48] 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."[49] Another RAT campaign labeled GhostShell, potentially linked to Iran, was discovered in July 2021 targeting aerospace and telecommunications companies, mainly in the Middle East.[50]

In August 2020, a presentation at the Blackhat USA 2020 conference outlined multiple examples of insecure internet communications traveling over satellite links.[51] 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. In 2022, researchers demonstrated the ability to broadcast a signal through the unused portion of a commercial satellite being decommissioned in GEO, highlighting the lack of authentication and controls on many older satellites.[52] In August 2022, another hacker demonstrated how to use physical access to a Starlink terminal to bypass security measures and access protected software, and potentially the ability to upload custom firmware.[53]

43 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.

44 Ibid.

45 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/.

46 Ruben Santamarta, "A Wake-Up Call for SATCOM Security," *IOActive*, 2014, https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf; Office of Inspector General, "Significant Security Deficiencies in NOAA's Information Systems Create Risks in Its National Critical Mission," Office of Inspector General, U.S. Department of Commerce, OIG-14-025-A, July 15, 2014, https://www.oig.doc.gov/Pages/Significant-Security-Deficiencies-in-NOAA-Information-Systems-Create-Risks-in-Its-National-Critical-Mission.aspx. 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/publications/the-world-today/2016-02/satellites-floating-targets.

47 CrowdStrike Intelligence Report: Putter Panda," *CrowdStrike*, June 9, 2014, https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf.

48 Ibid.

49 Ibid.

50 Cyberreason Nocturnus, "Operation Ghost-Shell: Novel RAT Targets Global Aerospace and Telecoms Firms," *Cyberreason*, October 6, 2021, https://www.cybereason.com/blog/operation-ghostshell-novel-rat-targets-global-aerospace-and-telecoms-firms.

51 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/.

52 Lily Hay Newman, "Researchers Used a Decommissioned Satellite to Broadcast Hacker TV," *Wired*, March 30, 2022. https://www.wired.com/story/satellite-hacking-anit-f1r-shadytel/.

53 Matt Burgess, "The Hacking of Starlink Terminals Has Begun," *Wired*, August 10, 2022, https://www.wired.com/story/starlink-internet-dish-hack/.

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 the 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.[54] 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.[55] This approach allows the hacker to anonymize Internet connections, impersonate legitimate high-speed Internet users, spoof DNS requests, and gain access to private networks.[56] When used as an anonymizer for subsequent attacks against high-value targets, this approach makes it very difficult for network analysts and law enforcement agencies to correctly attribute operations, or to locate and disable command servers.[57] 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.[58] 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.[59] 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.[60]

The fifth category is cyber attacks against satellites themselves, either using signals broadcast from ground antennas or perhaps from another satellite in close proximity. While there are no publicly known real-world cyber attacks in this category, researchers have started to explore this possibility. In August 2020, the US Air Force launched the "Hack-A-Sat" competition where individuals can compete to try and find vulnerabilities in software simulations of satellites.[61] In 2023, the Hack-A-Sat contest progressed to attacking the real world Moonlighter satellite in orbit.[62] In April 2023, the European Space Agency set up its own "ethical hacking exercise" at the third Cybersecurity for the Space Industry (CYSAT) conference in Paris, France, and used a ground test bench to simulate an operational OPS-SAT.[63] Attacking teams worked to try and breach different subsystems, including attitude control and an onboard camera.

A paper presented at the annual Blackhat USA conference in August 2023 also explored the many potential cyber security weaknesses of academic and scientific cubesats against malicious hacking from the ground and also found that commercial satellite developers were unaware of common cyber security practices.[64]

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.[65] 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.

Specific National Cyber Counterspace Capabilities

There are no documented cases of the United States conducting cyber attacks against other country's space systems. However, the United States very likely has among the most sophisticated cyber counterspace capabilities of any country, and declassified official documents hinting at such, under the category

54 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/.

55 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.

56 Ibid.

57 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/.

58 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.

59 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/.

60 Ibid.

61 Alyk Russell Kenlan, "The Air Force challenged hackers to break into a DOD satellite," *Air and Space Forces Magazine*, August 10, 2020, https://www.airandspaceforces.com/the-air-force-challenged-hackers-to-break-into-a-dod-satellite/.

62 Theresa Hitchens, "Italian team wins Space Force's first on-orbit Hack-A-Sat contest," *Breaking Defense*, August 15, 2023, https://breakingdefense.com/2023/08/italian-team-wins-space-forces-first-on-orbit-hack-a-sat-contest/.

63 "Thales seizes control of ESA demonstration satellite in first cybersecurity exercise of its kind," Thales Group, April 25, 2023, https://www.thalesgroup.com/en/worldwide/security/press_release/thales-seizes-control-esa-demonstration-satellite-first.

64 Johannes Willbold, "Houston, we have a problem: Analyzing the security of low Earth orbit satellites," paper presented at Blackhat USA 2023, August 10, 2023, https://www.blackhat.com/us-23/briefings/schedule/#houston-we-have-a-problem-analyzing-the-security-of-low-earth-orbit-satellites-32468.

65 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.

of "electronic nullification" date back to at least the Ford Administration in 1976. A recent hint at US capabilities comes in a news report from February 2024 that the Central Intelligence Agency (CIA) had established a secret base in Ukraine from which it has engaged in widespread attacks on Russian, Chinese, and Belarussian satellites to intercept the communications they carry.[66]

In February 2019, multiple anonymous sources claimed that the United States had an ongoing program of offensive cyber attacks aimed at undermining Iran's ballistic missile program.[67] 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.

While little information is publicly available regarding Russian cyberattacks targeted at space assets other than Viasat, 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 US-German ROSAT deep-space monitoring satellite, then issued commands for it to rotate toward the sun, frying its optics and rendering it useless.[68] More recently, since the end of 2015, Russia has engaged in a coordinated, escalating cyber attack campaign 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.[69] Most notably, this campaign included the physical incapacitation of Ukrainian power grids.[70] 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.[71] As part of its ongoing war against Ukraine since February 2022, Russia has systematically attacked the Ukrainian power grid with destructive weapons.[72]

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 US 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.[73] 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.[74] Given these examples and many others, there is no reason to believe that Russia is incapable of conducting similar operations in the space domain.

Several known and suspected Chinese cyber attacks against space systems were mentioned previously in this chapter. It is likely that China possesses significant cyber counterspace capabilities in addition to these known incidents, and is developing more. One hint comes from a CIA document leaked to the press in April 2023 that states China is building sophisticated cyber weapons to seize control of satellites during wartime.[75]

66 Adam Entous and Michael Schwirtz, "The Spy War: How the CIA secretly helps Ukraine fight Putin," *The New York Times*, February 25, 2024, https://www.nytimes.com/2024/02/25/world/europe/cia-ukraine-intelligence-russia-war.html.

67 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.

68 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.

69 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/.

70 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/.

71 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.

72 Joseph Majkut and Allegra Dawes, "Responding to Russian Attacks on Ukraine's Power Sector," Center for Strategic and International Studies, November 8, 2022, https://www.csis.org/analysis/responding-russian-attacks-ukraines-power-sector.

73 "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.

74 "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.

75 Mehul Srivastava, Felicia Schwartz, and Demetri Sevastopulo, "China building cyberweapons to hijack enemy satellites, says US leak," Arstechnica, April 21, 2023, https://arstechnica.com/information-technology/2023/04/china-building-cyberweapons-to-hijack-enemy-satellites-says-us-leak/.

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 US banks causing tens of millions of dollars in losses.[76] 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.[77] 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.[78] 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.[79] In early 2018, cybersecurity firm Symantec announced that "Chafer," an Iran-based hacking group believed largely due to its choice of targets to be government-affiliated, had successfully penetrated a range of targets including defense contractors, aviation firms, 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 US National Security Agency (NSA) in 2017 by a third party.[80] 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.

76 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.

77 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.

78 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.

79 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.

80 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.

North Korea's cyber capabilities appear to be even more sophisticated, and are likely to continue advancing rapidly, absent significant disruption on the Peninsula.[81] 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; [82] hacks of US and South Korean civilian critical infrastructure and military networks, with outcomes ranging from insertion of digital kill-switches intended to paralyze power supplies on-demand to successful theft of war plans; [83] 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; [84] and frequent and sustained cyber-espionage and cyber crime campaigns targeted at, among other things, large banks and financial institutions,[85] cryptocurrency exchanges,[86] and defense and defense-adjacent companies.[87] Many of these capabilities, especially those highlighted in the WannaCry incident, could cause tremendous damage if targeted at terrestrial infrastructure supporting space operations. Other cyber tools and techniques with counter-space implications likely either already exist or will in the not-too-distant future.

Potential Military Utility /

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

The first advantage is the flexibility and nature of producible effects. Extant cyber and electronic warfare capabilities can produce a range of effects, including theft, alteration, or denial of information, as well as control or destruction of satellites, their subcomponents, or supporting infrastructure. This allows the type and degree of counter-space operation to be narrowly tailored to the desired objective, in contrast to the comparatively blunt and single-note 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.[88]

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 can attend such deliberately opaque approaches, as the difficulty of guaranteeing a reliable and proportional response can create structural incentives for each side to move first in the event of an impending crisis.[89] 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

81 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.

82 Ibid.

83 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.

84 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.

85 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.

86 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.

87 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/.

88 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.

89 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.

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 the 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.[90] 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.[91] 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 have both 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.[92]

The March 2022 cyber attack against Viasat exemplifies all of these advantages and disadvantages. It was on the surface an extremely successful, and relatively low-cost, attack that was expertly timed to synchronize with a joint combined arms offensive and eliminate a critical space service in order to cripple Ukrainian defenses. However, there is mixed evidence as to its actual impact on the military operation and unlikely that those impacts lasted more than a few weeks into the war. Within a month of the attack, Ukraine had procured access to another satellite broadband communications system, Starlink, that has so far proven much more resistant to cyber attacks.

90 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.

91 “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.

92 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.

Appendix
One

HISTORICAL ANTI-SATELLITE TESTS IN SPACE

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 the kill vehicle.

TABLE 15-1 — HISTORICAL US ASAT TESTS IN SPACE

DATE	ASAT SYSTEM	ASAT TYPE	LAUNCH SITE	TARGET	NOTES
Sept. 22, 1959	High Virgo (TX-20)	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)
Oct. 1, 1961	SIP (NOTS-EV-2)	Direct Ascent	San Nicholas Island	None	Successful rocket test
Oct. 5, 1961	HiHo (NOTS-EV-1)	Direct Ascent	F4D-I	None	Rocket failure
Mar. 26, 1962	HiHo (NOTS-EV-1)	Direct Ascent	F4D-I	None	Rocket failure
May 5, 1962	SIP (NOTS-EV-2)	Direct Ascent	San Nicholas Island	None	Successful rocket test
Aug. 26, 1962	HiHo (NOTS-EV-1)	Direct Ascent	F4-C	None	Successful rocket test
Dec. 17, 1962	Program 505 (Nike Zeus)	Direct Ascent	WSMR	None	Success (reached designated point in space)
Feb. 15, 1963	Program 505 (Nike Zeus)	Direct Ascent	Kwajalein	None	Successful intercept of designated point in space
Mar. 21, 1963	Program 505 (Nike Zeus)	Direct Ascent	Kwajalein	None	Unsuccessful attempt to intercept simulated satellite target
Apr. 19, 1963	Program 505 (Nike Zeus)	Direct Ascent	Kwajalein	None	Unsuccessful attempt to intercept simulated satellite target
May 24, 1963	Program 505 (Nike Zeus)	Direct Ascent	Kwajalein	Agena D	Successful close intercept
Jan. 4, 1964	Program 505 (Nike Zeus)	Direct Ascent	Kwajalein	None	Successful intercept of a simulated satellite target
Feb. 14, 1964	Program 437 (Thor)	Direct Ascent	Johnston Atoll	Transit 2A Rocket Body	Success (passed within kill radius)
Mar. 1, 1964	Program 437 (Thor)	Direct Ascent	Johnston Atoll	Unknown	Success (primary missile scrubbed, backup missile passed within kill radius)
Apr. 21, 1964	Program 437 (Thor)	Direct Ascent	Johnston Atoll	Unknown	Success (passed within kill radius)
May 28, 1964	Program 437 (Thor)	Direct Ascent	Johnston Atoll	Unknown	Failed (missed intercept point)
Nov. 16, 1964	Program 437 (Thor)	Direct Ascent	Johnston Atoll	Unknown	Successful Combat Test Launch (passed within kill radius)
March 1965	Program 505 (Nike Zeus)	Direct Ascent	Kwajalein	None	–
Apr. 5, 1965	Program 437 (Thor)	Direct Ascent	Johnston Atoll	Transit 2A Rocket Body	Successful Combat Test Launch (passed within kill radius)
June-July 1965	Program 505 (Nike Zeus)	Direct Ascent	Kwajalein	None	Four test intercepts, of which three were successful
Jan. 13, 1966	Program 505 (Nike Zeus)	Direct Ascent	Kwajalein	None	Successful intercept with simulated target
Mar. 30, 1967	Program 437 (Thor)	Direct Ascent	Johnston Atoll	Unknown piece of space debris	Successful Combat Evaluation Launch (passed within kill radius)
May 15, 1968	Program 437 (Thor)	Direct Ascent	Johnston Atoll	Unknown	Successful Combat Evaluation Launch (passed within kill radius)
Nov. 21, 1968	Program 437 (Thor)	Direct Ascent	Johnston Atoll	Unknown	Successful Combat Evaluation Launch (passed within kill radius)
Mar. 28, 1970	Program 437 (Thor)	Direct Ascent	Johnston Atoll	Unknown satellite	Success (passed within kill radius)
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
Sept. 5, 1986	Delta 180 PAS	Co-Orbital	Cape Canaveral	Delta 2 R/B	Successful collision, debris generated
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
Feb. 20, 2008	SM-3	Direct Ascent	USS Lake Erie	USA 193	Successful test, debris generated

TABLE 15-2 — HISTORICAL RUSSIAN ASAT TESTS IN SPACE

DATE	ASAT SYSTEM	ASAT TYPE	LAUNCH SITE	TARGET	NOTES
Nov. 1, 1963	Polyot 1	Co-orbital	Baikonur	None	Engine and maneuvering test
Apr. 12, 1964	Polyot 2	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
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-M	Co-orbital	Baikonur	Cosmos 970	Successful intercept, debris created
Apr. 18, 1980	IS-M	Co-orbital	Baikonur	Cosmos 1171	Unsuccessful intercept, debris created
Feb. 2, 1981	IS-M	Co-orbital	Baikonur	Cosmos 1241	Two failed intercepts, no debris created
June 18, 1982	IS-M	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	None	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	Central Russia	None	Rocket test (successful)
Oct. 30, 2017	Cosmos 2521 (Burevestnik?)	Co-orbital	–	–	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
September 2019?	Cosmos 2536 (Burevestnik?)	Co-orbital	Plesetsk	Cosmos 2535	High speed RPO pass, potential ASAT test or collision
Apr. 15, 2020	Nudol	Direct Ascent	Plesetsk	None	Potential intercept, debris created
July 15, 2020	Cosmos 2536 Burevestnik?	Co-orbital	Plesetsk	None	Released subsatellite at relatively high speed
Dec. 16, 2020	Nudol	Direct Ascent	Plesetsk	None	Potential KKV, no intercept
April 2021	Nudol	Direct Ascent	Plesetsk	None	Unknown
Nov. 15, 2021	Nudol	Direct Ascent	Plesetsk	Cosmos 1408	Successful intercept, debris created

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

TABLE 15-3 — HISTORICAL CHINESE ASAT TESTS IN SPACE

DATE	ASAT SYSTEM	ASAT TYPE	LAUNCH SITE	TARGET	NOTES
July 5, 2005	SC-19	Direct Ascent	Xichang	None known	Likely rocket test
Feb. 6, 2006	SC-19	Direct Ascent	Xichang	None known	Likely near-miss of orbital target
Jan. 11, 2007	SC-19	Direct Ascent	Xichang	FY-1C satellite	Destruction of orbital target, debris created
Jan. 11, 2010	SC-19	Direct Ascent	Korla	CSS-X-11 ballistic missile launched from Jiuquan	Destruction of target
Jan. 27, 2013	Possible SC-19	Direct Ascent	Korla	Unknown ballistic missile launched from Jiuquan	Destruction of target
May 13, 2013	Possible DN-2	Direct Ascent	Xichang	None known	Likely rocket test
July 23, 2014	Possible DN-2	Direct Ascent	Korla? (Jiuquan?)	Likely ballistic missile launched from Jiuquan	Likely intercept test
Oct. 30, 2015	Possible DN-3	Direct Ascent	Korla	None known, possible ballistic missile	Likely rocket test
July 23, 2017	Possible DN-3	Direct Ascent	Jiuquan?	Likely ballistic missile	Likely intercept test
Feb. 5, 2018	Possible DN-3	Direct Ascent	Korla	CSS-5 ballistic missile	Likely intercept test
Feb. 4, 2021	Possible DN-3	Korla	Likely ballistic missile	Suborbital	Likely intercept test
Jun. 21, 2022	Possible DN-3	Korla	Likely ballistic missile	Suborbital	Likely intercept test

TABLE 15-4 — 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 created

Appendix
Two

16

IMAGERY OF COUNTER-SPACE RELATED FACILI-TIES

LAUNCH COMPLEXES /

UNITED STATES >
Fort Greely

63.953987°N -145.725365°W
(GBI Silos—image shown)

FIGURE 16-1 — FORT GREELY GBI FIELD

Fort Greely, located in Alaska, possesses 40 silos for the GBI missile, the interceptor component for the GMD system.

Function: ABM Field

Associated Programs: GBI

Key Dates: —

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)

FIGURE 16-2 — VANDENBERG SPACE LAUNCH COMPLEX 6

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.

Function: Space Launch Complex

Associated Programs: —

Key Dates: —

LAUNCH COMPLEXES /

UNITED STATES >
Cape Canaveral

28.583414°N -80.582891°W
(SLC 41)

28.532311°N -80.566601°W
(SLC 37)

28.532311°N -80.566601°W
(X-37B Hangar—image shown)

FIGURE 16-3 — CAPE CANAVERAL X-37B HANGAR

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.

Function: Space Launch Complex

Associated Programs: X-37B

Key Dates: —

LAUNCH COMPLEXES /

RUSSIA >
Kapustin Yar

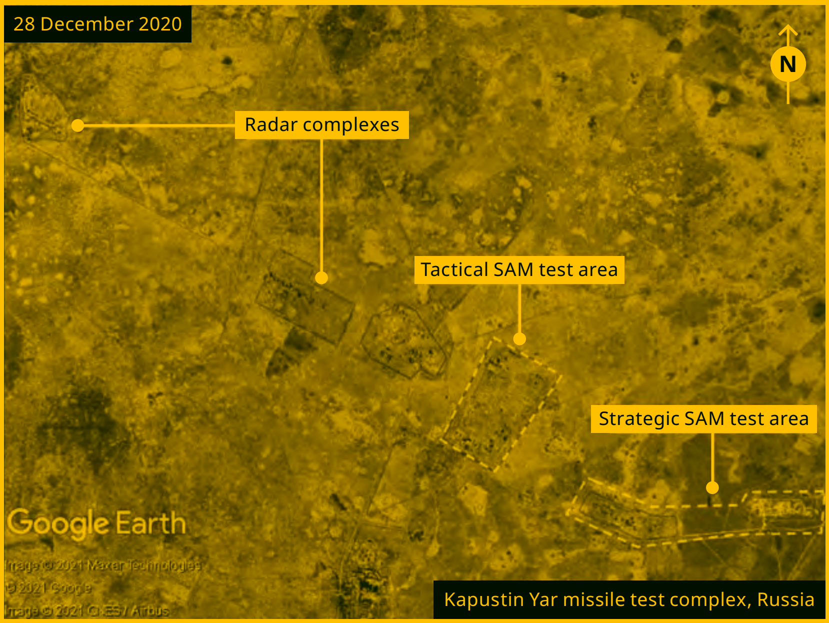
48.794055°N 45.734890°E
(SAM test complex)

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)

FIGURE 16-4 — KAPUSTIN YAR MOBILE MISSILE LAUNCH SITE



Kapustin Yar missile test complex, Russia

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.

Function: Missile test and training complex

Associated Programs: Nudol

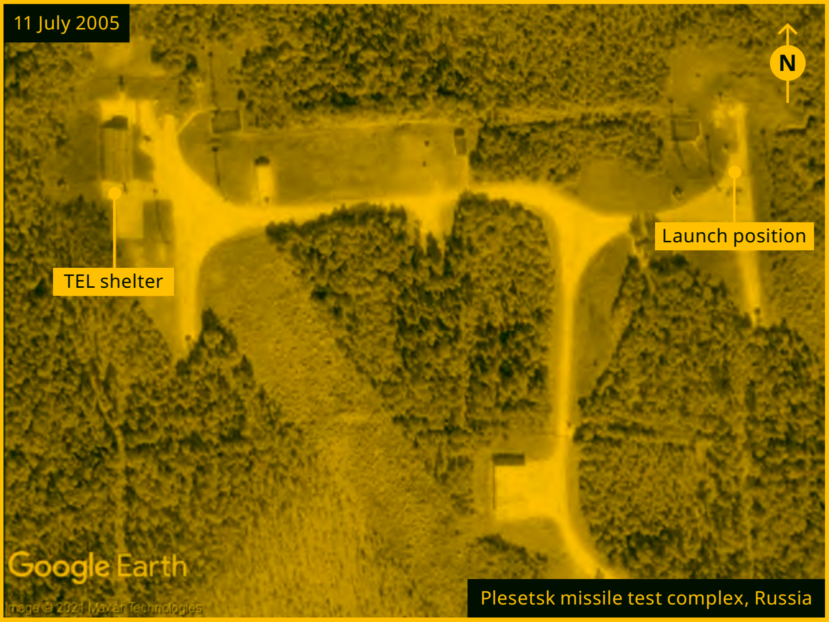
Key Dates:

December 16, 2016
(Possible Nudol ASAT test)

RUSSIA >
Plesetsk

63.008092°N 41.551308°E
(Mobile missile launch complex—image shown)

FIGURE 16-5 — 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.

Function: Missile launch complex

Associated Programs: Nudol

Key Dates:

August 12, 2014
(Nudol ASAT test)

April 22, 2015
(Nudol ASAT test)

November 18, 2015
(Nudol ASAT test)

May 25, 2016
(Nudol ASAT test)

November 15, 2021
(Nudol ASAT test)

LAUNCH COMPLEXES /

RUSSIA >
Plesetsk

62.887012°N 40.847235°E
(Site 133—image shown)

FIGURE 16-6 — PLESETSK SPACE LAUNCH CENTER SITE 133

Site 133 at Plesetsk contains the launch pad for the Rockot booster, which was used to launch the first set of Russian RPO payloads into LEO in 2013-2015.

Function: Space launch complex

Associated Programs: Nivelir

Key Dates:

November 20, 1990
(Potential Naryad-V launch)

December 20, 1991
(Potential Naryad-V launch)

December 26, 1994
(Potential Naryad-V launch)

December 25, 2013
(Launch of Cosmos 2491)

May 23, 2014
(Launch of Cosmos 2499)

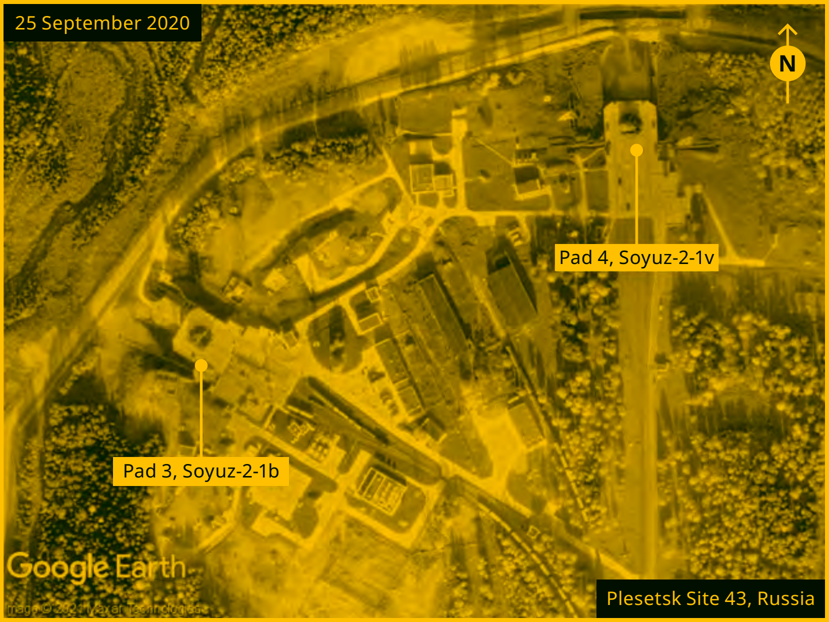
March 31, 2015
(Launch of Cosmos 2504)

LAUNCH COMPLEXES /

RUSSIA >
Plesetsk

62.927217°N 40.449530°E
(Site 43, Pads 3 and 4—image shown)

FIGURE 16-7 — 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.

Function: Space launch facility

Associated Programs: Nivelir, Burevestnik

Key Dates:

June 23, 2017
(Launch of Cosmos 2519)

July 10, 2019
(Launch of Cosmos 2535 and Cosmos 2536)

November 25, 2019
(Launch of Cosmos 2542)

LAUNCH COMPLEXES /

RUSSIA >
Plesetsk

62.769056°N 40.373730°E
(Burevestnik construction —image shown)

FIGURE 16-8 — PLESETSK AREA 141 BUREVESTNIK FACILITIES

Area 141 at Plesetsk is under construction to support the Burevestnik program, which is believed to include an air-launched co-orbital ASAT.

Function: Support facility

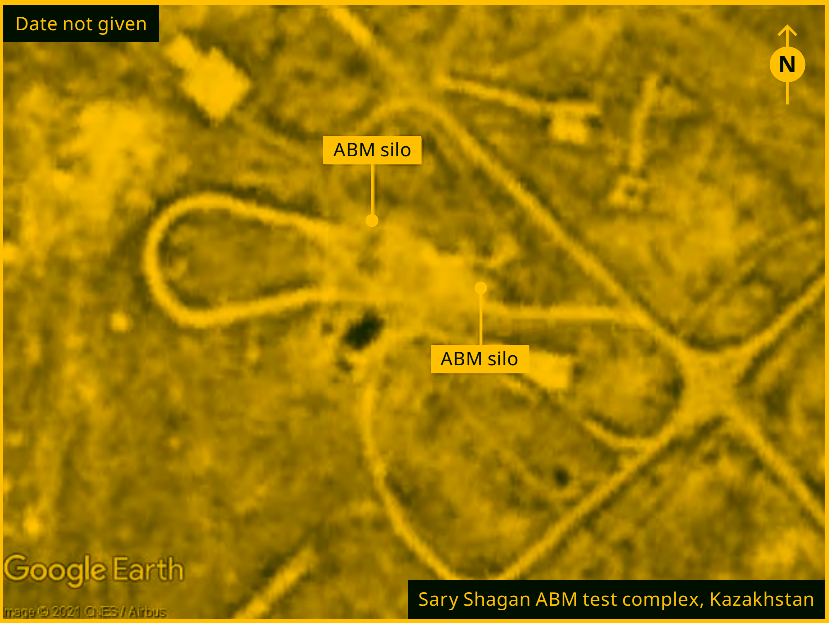
Associated Programs: Burevestnik

Key Dates: —

RUSSIA >
Sary Shagan

46.443219°N 72.849398°E
(Site 35 ABM test complex—image shown)

FIGURE 16-9 — 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.

Function:
Support facility

Associated Programs: 51T6, 53T6, 53T6M

Key Dates:

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)

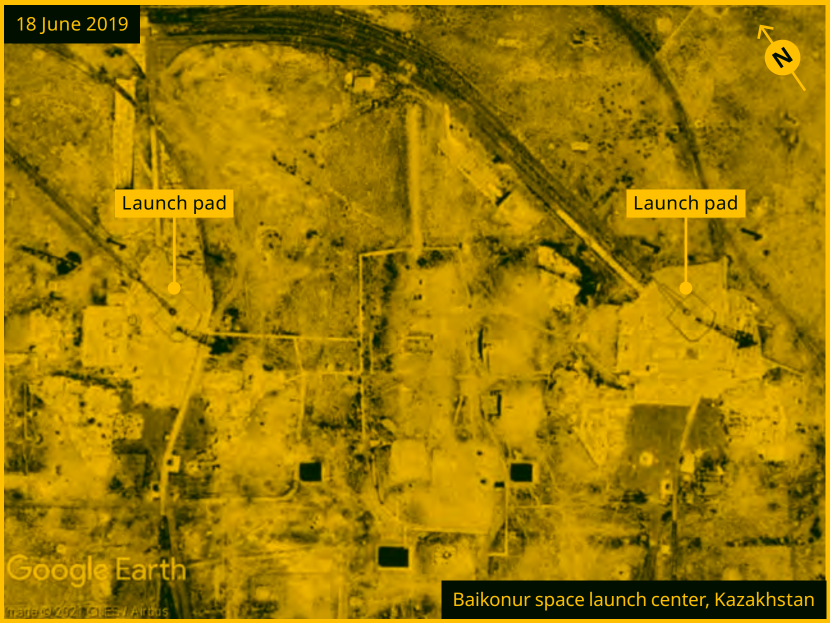
June 16, 2017
(ABM test launch, 53T6 or 53T6M)

LAUNCH COMPLEXES /

RUSSIA >
Baikonur

46.079749°N 62.932500°E
(Site 90, IS launch complex—image shown)

FIGURE 16-10 — BAIKONUR COSMODROME SITE 90



Baikonur space launch center, Kazakhstan

While the Baikonur Cosmodrome in Kazakhstan is most famous as the historical launch site for Russia's human spaceflight program, it has also supported many 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.

Function: Space launch complex

Associated Programs: IS, IS-M

Key Dates:

October 27, 1967
(First test launch of IS ASAT)

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

LAUNCH COMPLEXES /

CHINA >
Jiuquan

41.281777°N 100.306390°E
(ASAT/ABM target launch site—image shown)

FIGURE 16-11 — JIUQUAN SUBORBITAL LAUNCH COMPLEX

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 that may be used to launch suborbital targets for ASAT testing.

Function: Missile launch complex

Associated Programs: SC-19, DN-1, DN-3

Key Dates:

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)

LAUNCH COMPLEXES /

CHINA >
Korla West

41.537300°N 86.353317°E
(Garrison complex—image shown)

41.537667°N 86.372073°E
(ABM/ASAT launch pad)

FIGURE 16-12 — KORLA WEST GARISSON 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.

Function: ASAT complex

Associated Programs: SC-19/DN-1, DN-3

Key Dates:

January 11, 2010
(SC-19 ASAT test)

January 20, 2013
(SC-19 ASAT test)

July 23, 2014
(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)

LAUNCH COMPLEXES /

CHINA >
Korla West

41.537667°N 86.372073°E
(ABM/ASAT launch pad—image shown)

FIGURE 16-13 — 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.

Function: —

Associated Programs: —

Key Dates:

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)

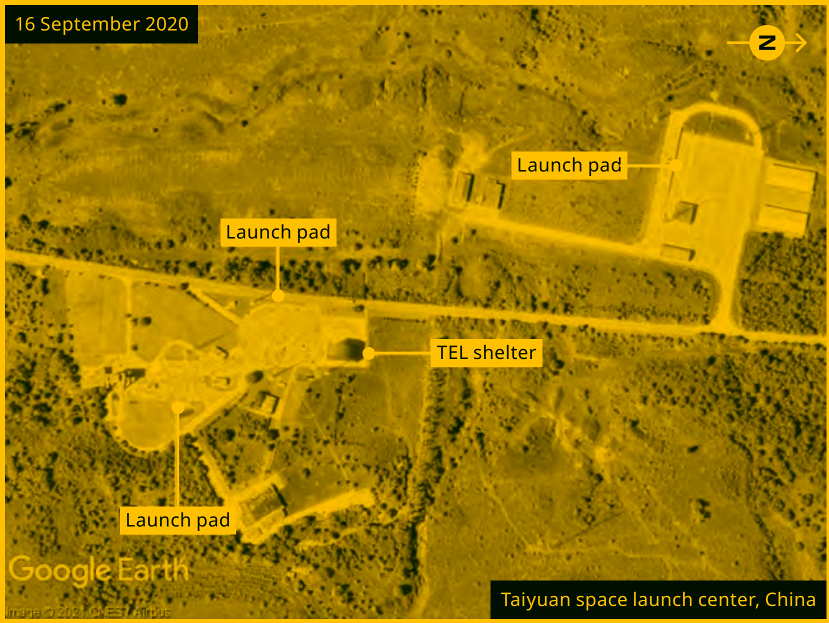
July 23, 2017
(DN-3 ASAT test)

LAUNCH COMPLEXES /

CHINA >
Taiyuan

38.840519°N 111.604648°E
(Possible ASAT/ABM target launch site—image shown)

FIGURE 16-14 — 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 one 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.

Function: Missile test complex

Associated Programs: DN-3

Key Dates:

December 9, 2016
(Possible target launch supporting DN-3 launch from Korla)

July 23, 2017
(Possible target launch supporting DN-3 launch from Korla)

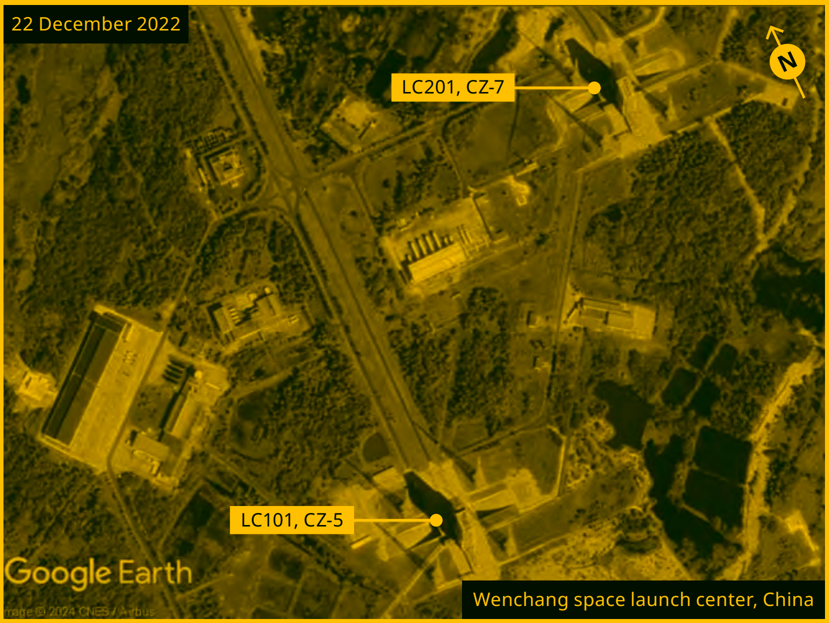
LAUNCH COMPLEXES /

CHINA >
Wenchang

19.614533°N 110.951151°E
(LM-5 launch pad)

19.618657°N 110.955415°E
(LM-7 launch pad)

FIGURE 16-15 — WENCHANG SPACE LAUNCH CENTER



Wenchang Space Launch Center on the island of Hainan is China's newest space launch complex, with the benefits of being nearest to the Equator and a greater range of allowable launch azimuths.

Function: Space launch complex

Associated Programs: SJ-23

Key Dates:

January 18, 2023
Launch of SJ-23 to GEO

LAUNCH COMPLEXES /

CHINA >
Xichang

28.249140°N 102.022942°E
(Northern ABM/ASAT and target launch pad—image shown)

FIGURE 16-16 — 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 ongoing construction.

Function: Missile test complex

Associated Programs: SC-19

Key Dates:

July 5, 2005
(SC-19 ASAT test)

February 6, 2006
(SC-19 ASAT test)

January 11, 2007
(SC-19 ASAT test)

LAUNCH COMPLEXES /

CHINA >
Xichang

28.242775°N 102.032946°E
(Southern ABM/ASAT and target launch pad—image shown)

FIGURE 16-17 — 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 ASAT test on May 13, 2013, that went nearly to GEO.

Function: Missile test complex

Associated Programs: DN-2

Key Dates:

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)

LAUNCH COMPLEXES /

INDIA >
Satish Dhawan

13.733280°N 80.234840°E
(First Launch Pad—image shown)

13.719751°N 80.230431°E
(Second Launch Pad)

FIGURE 16-18 — SATISH DHAWAN SPACE CENTRE

Satish Dhawan Space Centre, located in Sriharikota in Andhra Pradesh, is India's primary space launch center.

Function: Space launch complex

Associated Programs: PSLV

Key Dates: —

LAUNCH COMPLEXES /

INDIA >
Abdul Kalam Island

20.755135°N 87.088511°E
(Launch Complex IV—image shown)

FIGURE 16-19 — ABDUL KALAM ISLAND LAUNCH COMPLEX

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.

Function: Missile test complex

Associated Programs: PDV

Key Dates:

February 12, 2019
(Unsuccessful DA-ASAT test)

March 27, 2019
(Successful DA-ASAT test)

LAUNCH COMPLEXES /

IRAN >
Semnan

35.23472°N 53.92083°E
(Safir Launch Pad—image shown)

35.2583°N 53.9547°E
(Imam Khomeini Spaceport)

FIGURE 16-20 — 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.

Function: Space launch complex

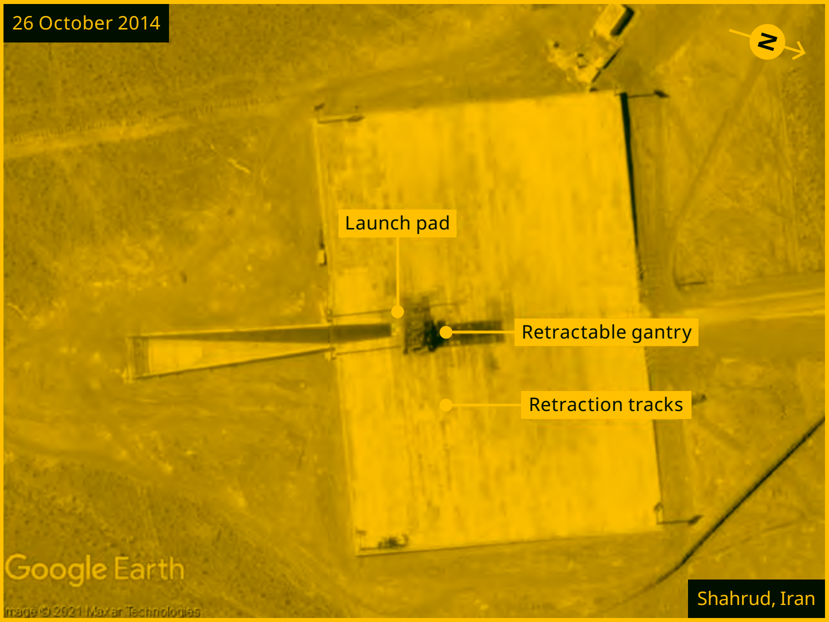
Associated Programs: Safir, Simorgh

Key Dates: —

IRAN >
Shahrud

36.200599°N 055.333928°E

FIGURE 16-21 — SHAHRUD LAUNCH SITE



Shahrud space launch facility was built approximately 40 kilometers SE from the town of Shahrud in Semnan province and appears to be the launch site for Iran's military space launches.

Function: Space launch complex

Associated Programs: Qassed

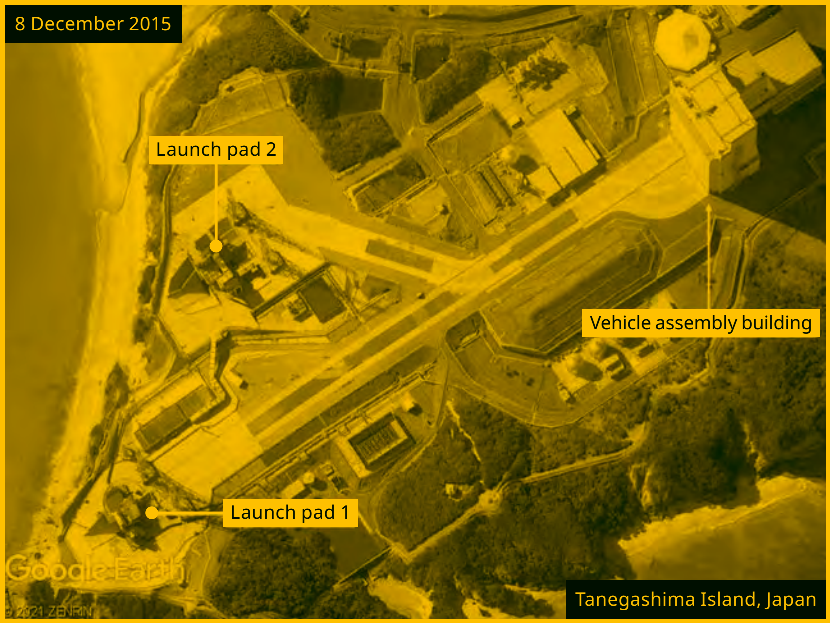
Key Dates: —

LAUNCH COMPLEXES /

JAPAN >
Tanegashima

30.402291°N 130.974102°E

FIGURE 16-22 — TANEGASHIMA SPACE CENTER



Tanegashima Space Center is Japan's largest space launch facility and is located on the southeast coast of Tanegashima island, just south of Kyushu.

Function: —

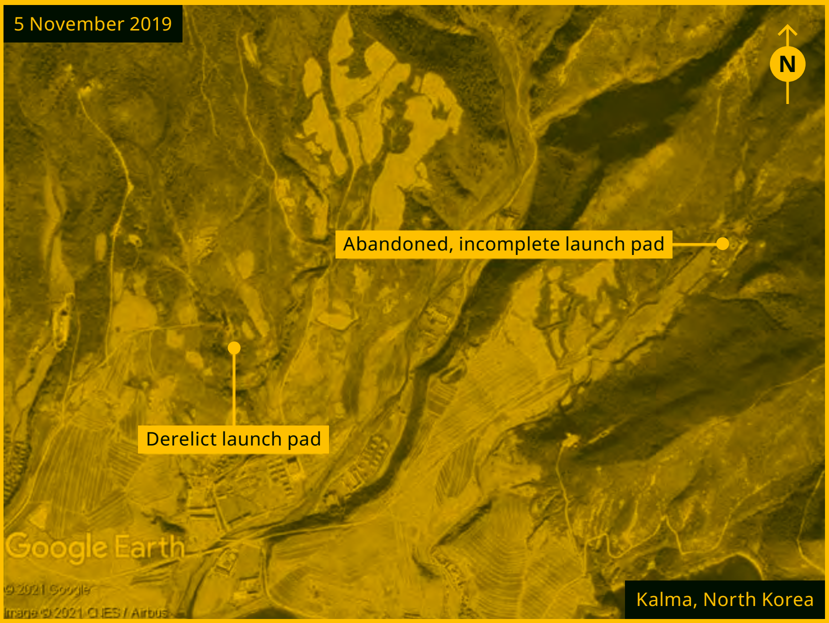
Associated Programs: —

Key Dates: —

NORTH KOREA >
Tonghae

40.85°N 129.666667°E

FIGURE 16-23 — TONGHAE SATELLITE LAUNCHING GROUND



Tonghae Satellite Launching Ground, also known as Musudan-ri, is a ballistic missile and space launch site in North Korea.

Function: Space launch complex

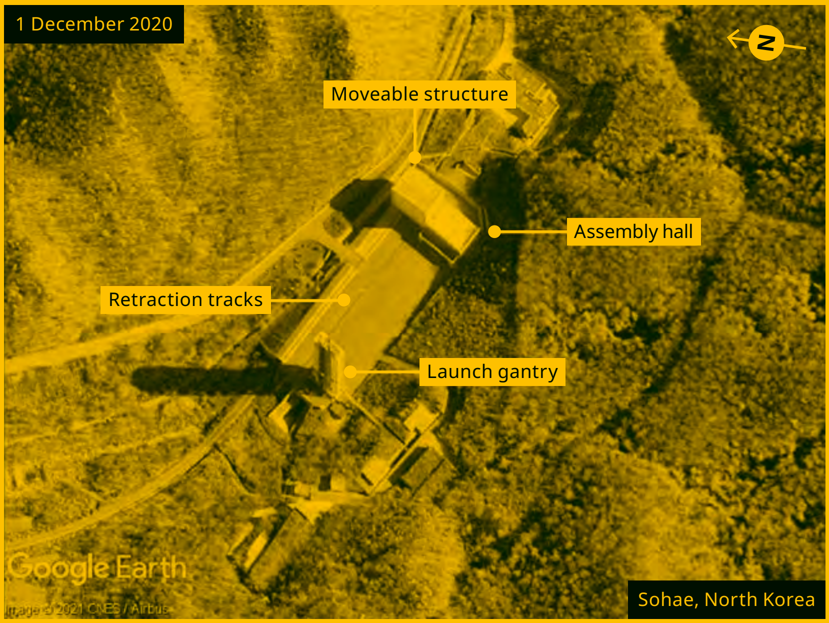
Associated Programs: TD-1

Key Dates: —

NORTH KOREA >
Sohae

39.660°N 124.705°E

FIGURE 16-24 — 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.

Function: Space launch complex

Associated Programs: Unha

Key Dates: —

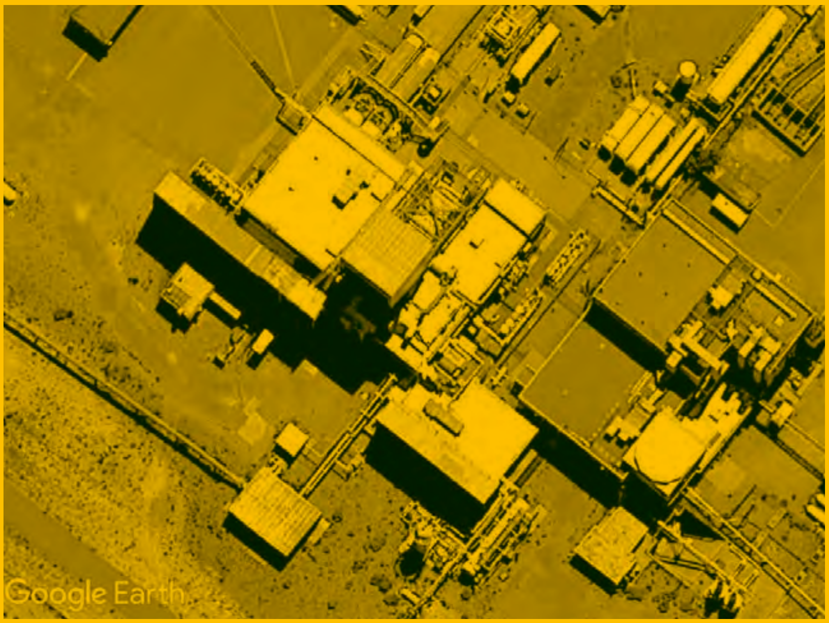
01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

DIRECTED ENERGY WEAPONS AND ELECTRONIC WARFARE COMPLEXES /

UNITED STATES >
Fixed laser sites

32.632037°N -106.333804°W

FIGURE 16-25 — MIRACL LASER



The Mid-Infrared Advanced Chemical Laser (MIRACL) is a megawatt-class laser weapon research and test facility located at White Sands Missile Range in New Mexico. It first became operational in 1980 and in 1997 was used to attempt to blind the MSTI-3 satellite in an Air Force test.

Function: Fixed laser site

Associated Programs: MIRACL

Key Dates: —

DIRECTED ENERGY WEAPONS AND ELECTRONIC WARFARE COMPLEXES /

RUSSIA >
Mobile laser deployment sites

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 16-26 — 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.

Function: Mobile laser deployment site

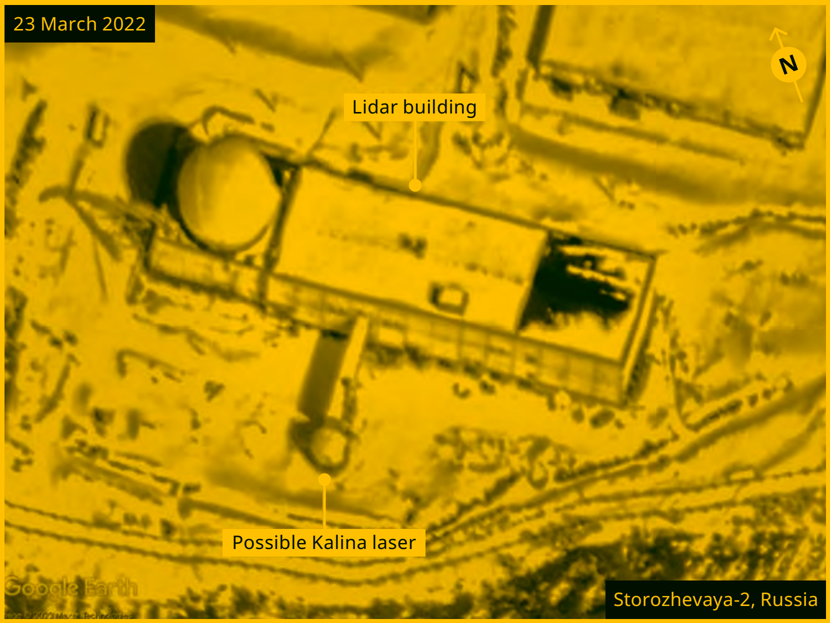
Associated Programs: Peresvet

Key Dates: —

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16

43.717130°N 041.227706°E

FIGURE 16-27 — KALINA LASER COMPLEX NEAR ZELENCHUKSKAYAUDE



Russia is constructing a new laser system called Kalina at the site of the Krona space surveillance complex, located several kilometers west of Zelenchukskaya.

Function: Fixed laser site

Associated Programs: Kalina

Key Dates: —

DIRECTED ENERGY WEAPONS AND ELECTRONIC WARFARE COMPLEXES /

RUSSIA >
Tobol Electronic Warfare sites

56.014836°N 38.006669°E
(8282/1—Shcholkovo)

51.856779°N 107.986240°E
(8282/3—Ulan-Ude—image shown)

44.019977°N 131.756142°E
(8282/4—Ussuriysk Primorskiy)

58.445332°N 092.269218°E
(8282/5—Yeniseisk)

54.939364°N 20.240636°E
(8282/6— Mobile site near Pionerskiy)

44.931381°N 40.989706°E
(8282/7— Mobile site near Armavir)

FIGURE 16-28 — TOBOL ELECTRONIC WARFARE COMPLEX NEAR ULAN-UDE

The Tobol complexes contain multiple satellite antennas that can be used for both offensive and defensive electronic warfare purposes. Two of the sites, 8282/6 near Pionerskiy and 8282/7 near Armavir, are parking locations for mobile sensors.

Function: Fixed EW complex

Associated Programs: Tobol

Key Dates: —

CHINA >
Laser test sites

31.532158°N 104.740708°E
(Mianyang—image shown)

31.901428°N 117.162222°E
(Hefei)

41.761422°N 87.418331°E
(Bohu)

34.7475°N 113.781767°E
(Zhengzhou)

43.790506°N 125.442814°E
(Changchun)

FIGURE 16-29 — 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.

Function: Fixed laser site

Associated Programs: —

Key Dates: —

DIRECTED ENERGY WEAPONS AND ELECTRONIC WARFARE COMPLEXES /

CHINA >
Laser test sites

31.532158°N 104.740708°E
(Mianyang)

31.901428°N 117.162222°E
(Hefei)

41.761422°N 87.418331°E
(Bohu—image shown)

34.7475°N 113.781767°E
(Zhengzhou)

43.790506°N 125.442814°E
(Changchun)

FIGURE 16-30 — 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.

Function: Fixed laser site

Associated Programs: —

Key Dates: —

SENSOR COMPLEXES /

UNITED STATES >
Space surveillance network

39.136111°N 121.350831°W
(Beale)

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)

70.36639722°N 31.12687500°E
(Globus II)

9.394789°N 167.47925°E
(Reagan Test Site)

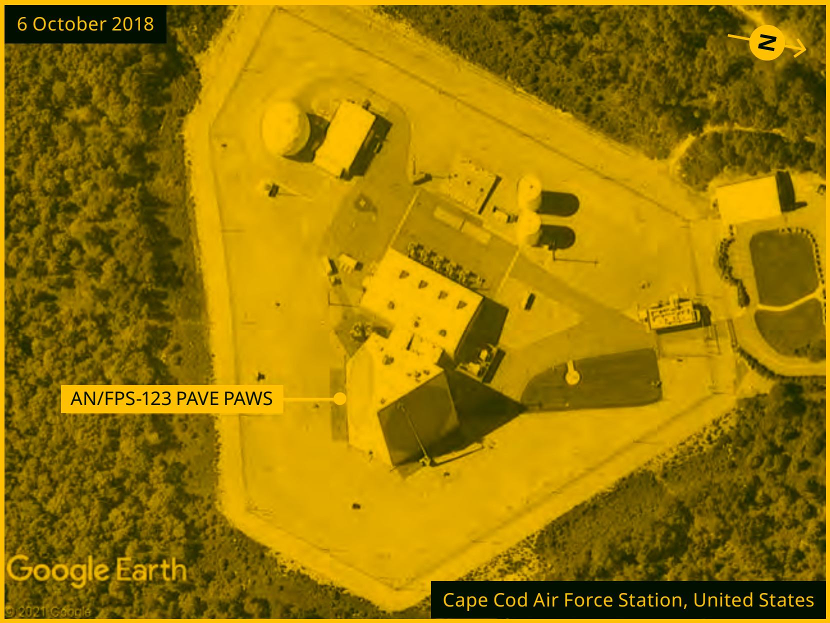
7.41227222°S 72.45240556°E
(GEODSS Diego Garcia)

21.816631°S 114.165617°E
(Holt C-Band Radar)

-21.895703°S 114.089939°E
(Space Surveillance Telescope)

20.7088°N 156.2578°W
(Air Force Maui Optical and Supercomputing Observatory)

FIGURE 16-31 — CAPE COD MISSILE WARNING RADAR



The US 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 Space Force Station in Massachusetts, from which it has coverage over much of the northeastern coast of the United States.

Function: Radar

Associated Programs: SSN

Key Dates: —

SENSOR COMPLEXES /

UNITED STATES >
Space surveillance network

39.136111°N 121.350831°W
(Beale)

41.752219°N 70.538061°W
(Cod)

76.570308°N 68.299256°W
(Thule)

64.290006°N 149.191381°W
(Clear)

54.3616°N 0.6697°W
(Fylingdales—image shown)

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)

70.36639722°N 31.12687500°E
(Globus II)

9.394789°N 167.47925°E
(Reagan Test Site)

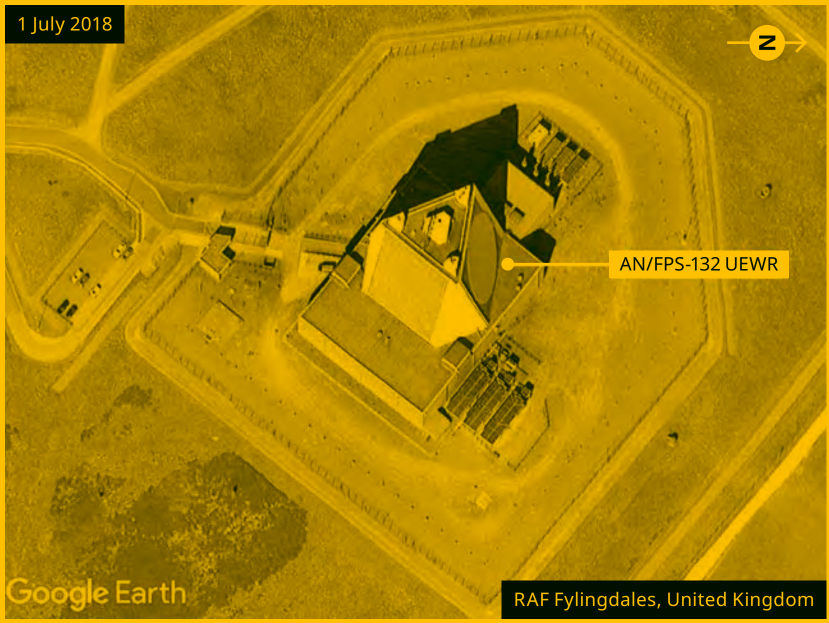
7.41227222°S 72.45240556°E
(GEODSS Diego Garcia)

21.816631°S 114.165617°E
(Holt C-Band Radar)

-21.895703°S 114.089939°E
(Space Surveillance Telescope)

20.7088°N 156.2578°W
(Air Force Maui Optical and
Supercomputing Observatory)

FIGURE 16-32 — FYLINGDALES MISSILE WARNING RADAR



The above image shows the AN/FPS-126 radar located at Royal Air Force (RAF) Fylingdales in North Yorkshire, England. Note that the RAF Fylingdales radar has three faces, giving it 360-degree coverage, compared to the two faces of the Cod radar.

Function: Radar

Associated Programs: SSN

Key Dates: —

SENSOR COMPLEXES /

UNITED STATES >
Space surveillance network

39.136111°N 121.350831°W
(Beale)

41.752219°N 70.538061°W
(Cod)

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—image shown)

8.723375°N 167.718564°E
(Space Fence)

42.620033°N 71.490289°W
(Lincoln Space Surveillance Complex)

70.36639722°N 31.12687500°E
(Globus II)

9.394789°N 167.47925°E
(Reagan Test Site)

7.41227222°S 72.45240556°E
(GEODSS Diego Garcia)

21.816631°S 114.165617°E
(Holt C-Band Radar)

-21.895703°S 114.089939°E
(Space Surveillance Telescope)

20.7088°N 156.2578°W
(Air Force Maui Optical and Supercomputing Observatory)

FIGURE 16-33 — 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.

Function: Radar

Associated Programs: SSN

Key Dates: —

SENSOR COMPLEXES /

UNITED STATES >
Space surveillance network

`39.136111°N 121.350831°W`
(Beale)

`41.752219°N 70.538061°W`
(Cod)

`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—image shown)

`42.620033°N 71.490289°W`
(Lincoln Space Surveillance Complex)

`70.36639722°N 31.12687500°E`
(Globus II)

`9.394789°N 167.47925°E`
(Reagan Test Site)

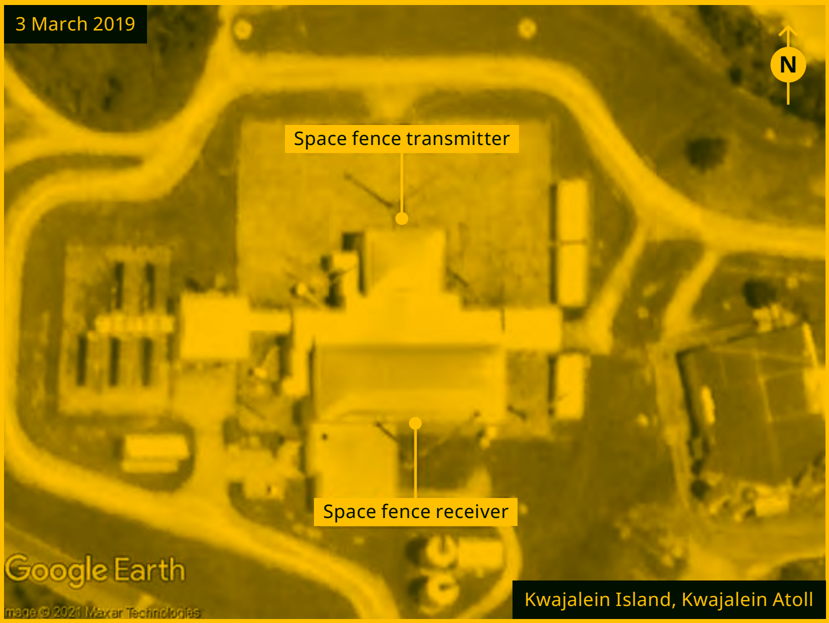
`7.41227222°S 72.45240556°E`
(GEODSS Diego Garcia)

`21.816631°S 114.165617°E`
(Holt C-Band Radar)

`-21.895703°S 114.089939°E`
(Space Surveillance Telescope)

`20.7088°N 156.2578°W`
(Air Force Maui Optical and Supercomputing Observatory)

FIGURE 16-34 — KWAJALEIN S-BAND SPACE FENCE



The above image shows the S-Band Space Fence located on Kwajalein Atoll in the South Pacific. This system became operational in 2020 and can track objects as small as a few centimeters in size out to 36,000 kilometers.

Function: Radar

Associated Programs: SSN

Key Dates: —

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

SENSOR COMPLEXES /

UNITED STATES >
Space surveillance network

39.136111°N 121.350831°W
(Beale)

41.752219°N 70.538061°W
(Cod)

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 —image shown)

70.36639722°N 31.12687500°E
(Globus II)

9.394789°N 167.47925°E
(Reagan Test Site)

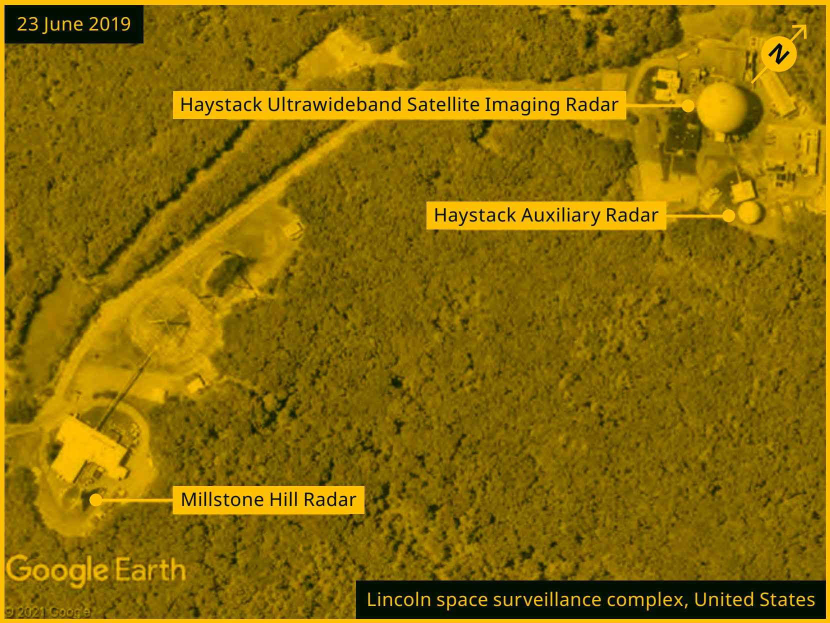
7.41227222°S 72.45240556°E
(GEODSS Diego Garcia)

21.816631°S 114.165617°E
(Holt C-Band Radar)

-21.895703°S 114.089939°E
(Space Surveillance Telescope)

20.7088°N 156.2578°W
(Air Force Maui Optical and Supercomputing Observatory)

FIGURE 16-35 — 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.

Function: Radar complex

Associated Programs: SSN

Key Dates: —

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16

SENSOR COMPLEXES /

UNITED STATES >
Space surveillance network

39.136111°N 121.350831°W
(Beale)

41.752219°N 70.538061°W
(Cod)

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)

70.36639722°N 31.12687500°E
(Globus II—image shown)

9.394789°N 167.47925°E
(Reagan Test Site)

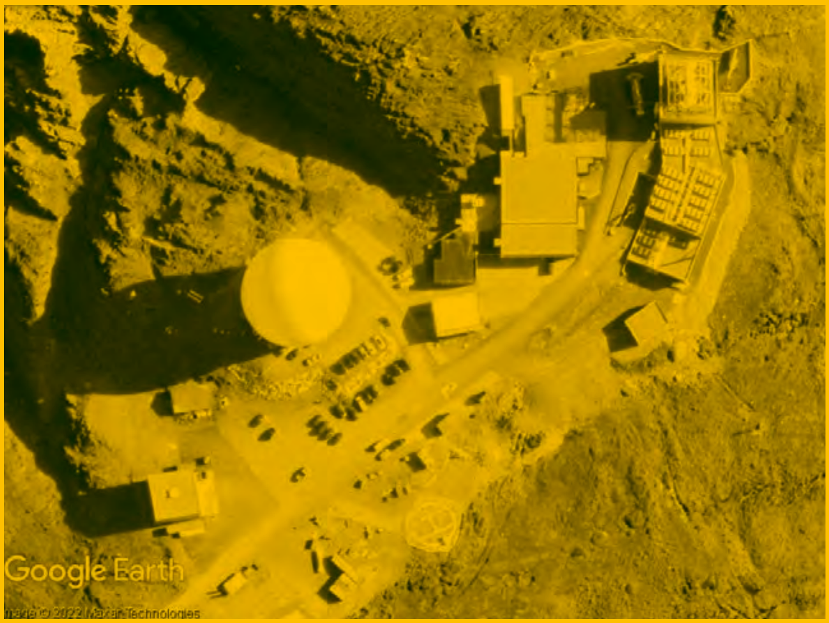
7.41227222°S 72.45240556°E
(GEODSS Diego Garcia)

21.816631°S 114.165617°E
(Holt C-Band Radar)

-21.895703°S 114.089939°E
(Space Surveillance Telescope)

20.7088°N 156.2578°W
(Air Force Maui Optical and Supercomputing Observatory)

FIGURE 16-36 — GLOBUS II RADAR



The above image shows the Globus II radar, located in Vardø, on the island of Vårberget in Norway. It is a single dish mechanical tracking radar for tracking and characterizing space objects out to 36,000 kilometers and contributes to the US SSN.

Function: Radar

Associated Programs: SSN

Key Dates: —

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

SENSOR COMPLEXES /

UNITED STATES >
Space surveillance network

39.136111°N 121.350831°W
(Beale)

41.752219°N 70.538061°W
(Cod)

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)

70.36639722°N 31.12687500°E
(Globus II)

9.394789°N 167.47925°E
(Reagan Test Site—image shown)

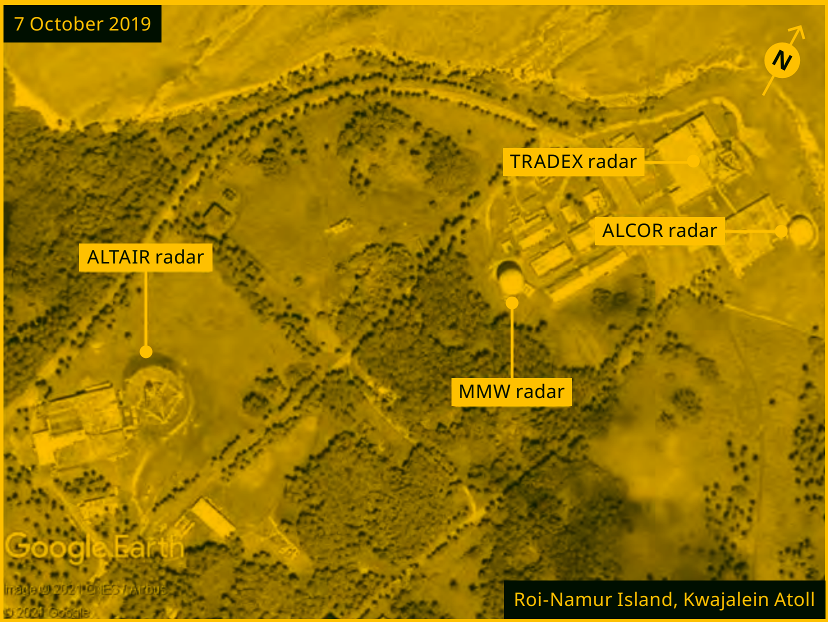
7.41227222°S 72.45240556°E
(GEODSS Diego Garcia)

21.816631°S 114.165617°E
(Holt C-Band Radar)

-21.895703°S 114.089939°E
(Space Surveillance Telescope)

20.7088°N 156.2578°W
(Air Force Maui Optical and Supercomputing Observatory)

FIGURE 16-37 — 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.

Function: Radar complex

Associated Programs: SSN

Key Dates: —

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

SENSOR COMPLEXES /

UNITED STATES >
Space surveillance network

39.136111°N 121.350831°W
(Beale)

41.752219°N 70.538061°W
(Cod)

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)

70.36639722°N 31.12687500°E
(Globus II)

9.394789°N 167.47925°E
(Reagan Test Site)

7.41227222°S 72.45240556°E
(GEODSS Diego Garcia—image shown)

21.816631°S 114.165617°E
(Holt C-Band Radar)

-21.895703°S 114.089939°E
(Space Surveillance Telescope)

20.7088°N 156.2578°W
(Air Force Maui Optical and Supercomputing Observatory)

FIGURE 16-38 — GEODSS DIEGO GARCIA

The above image shows the Ground-based Electro-Optical Deep Space Surveillance (GEODSS) complex located on Diego Garcia, British Indian Ocean Territory, which includes a 1-meter optical telescope. The Diego Garcia installation is one of three GEODSS sites, the other two are located in Socorro, New Mexico, and on the island of Maui, Hawaii.

Function: Optical telescope complex

Associated Programs: SSN

Key Dates: —

SENSOR COMPLEXES /

UNITED STATES >
Space surveillance network

39.136111°N 121.350831°W
(Beale)

41.752219°N 70.538061°W
(Cod)

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)

70.36639722°N 31.12687500°E
(Globus II)

9.394789°N 167.47925°E
(Reagan Test Site)

7.41227222°S 72.45240556°E
(GEODSS Diego Garcia)

21.816631°S 114.165617°E
(Holt C-Band Radar—image shown)

-21.895703°S 114.089939°E
(Space Surveillance Telescope)

20.7088°N 156.2578°W
(Air Force Maui Optical and Supercomputing Observatory)

FIGURE 16-39 — HOLT C-BAND RADAR IN EXMOUTH

The image above shows the C-Band radar moved from Antigua Island in the Atlantic to Naval Communication Station Harold E. Holt near Exmouth, Western Australia, to augment the SSN's coverage in the Southern Hemisphere.

Function: Radar

Associated Programs: SSN

Key Dates: —

SENSOR COMPLEXES /

UNITED STATES >
Space surveillance network

39.136111°N 121.350831°W
(Beale)

41.752219°N 70.538061°W
(Cod)

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)

70.36639722°N 31.12687500°E
(Globus II)

9.394789°N 167.47925°E
(Reagan Test Site)

7.41227222°S 72.45240556°E
(GEODSS Diego Garcia)

21.816631°S 114.165617°E
(Holt C-Band Radar)

-21.895703°S 114.089939°E
(Space Surveillance Telescope—image shown)

20.7088°N 156.2578°W
(Air Force Maui Optical and Supercomputing Observatory)

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16

FIGURE 16-40 — SPACE SURVEILLANCE TELESCOPE IN EXMOUTH

The image above shows the Space Surveillance Telescope (SST), which is a 3.5-meter wide field of view telescope originally developed by DARPA in New Mexico before being relocated to Naval Communication Station Harold E. Holt near Exmouth, Western Australia, to augment the SSN's coverage in the Southern Hemisphere.

Function: Optical telescope

Associated Programs: SSN

Key Dates: —

SENSOR COMPLEXES /

UNITED STATES >
Space surveillance network

39.136111°N 121.350831°W
(Beale)

41.752219°N 70.538061°W
(Cod)

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)

70.36639722°N 31.12687500°E
(Globus II)

9.394789°N 167.47925°E
(Reagan Test Site)

7.41227222°S 72.45240556°E
(GEODSS Diego Garcia)

21.816631°S 114.165617°E
(Holt C-Band Radar)

-21.895703°S 114.089939°E
(Space Surveillance Telescope)

20.7088°N 156.2578°W
(Air Force Maui Optical and Supercomputing Observatory—image shown)

FIGURE 16-41 — AIR FORCE MAUI OPTICAL AND SUPERCOMPUTING OBSERVATORY

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.

Function: Optical telescope complex

Associated Programs: SSN

Key Dates: —

SENSOR COMPLEXES /

RUSSIA >
Radar complexes

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)

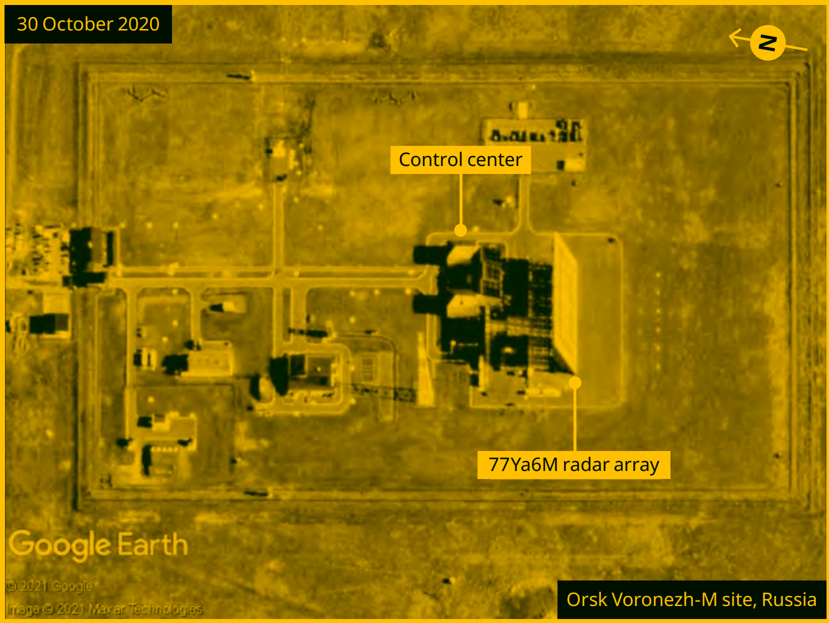
54.857482°N 20.182510°E
(77Ya6DM)

44.925428°N 40.983915°E
(77Ya6DM)

52.855571°N 103.232513°E
(77Ya6VP)

67.613910°N 63.752342°E
(under construction)

FIGURE 16-42 — VORONEZH RADAR AT ORSK



The image above shows the Voronezh-VP array near Orsk, one of several such radars in operational use or under construction.

Function: Radar

Associated Programs: Voronezh

Key Dates: —

SENSOR COMPLEXES /

RUSSIA >
Radar complexes

65.209966°N 57.285247°E
(Daryal—image shown)

52.848887°N 26.470524°E
(Volga)

FIGURE 16-43 — DARYAL RADAR AT PECHORA

The image above shows the Daryal bistatic array near Pechora.

Function: Radar

Associated Programs: Daryal/Volga

Key Dates: —

SENSOR COMPLEXES /

RUSSIA >
Radar complexes

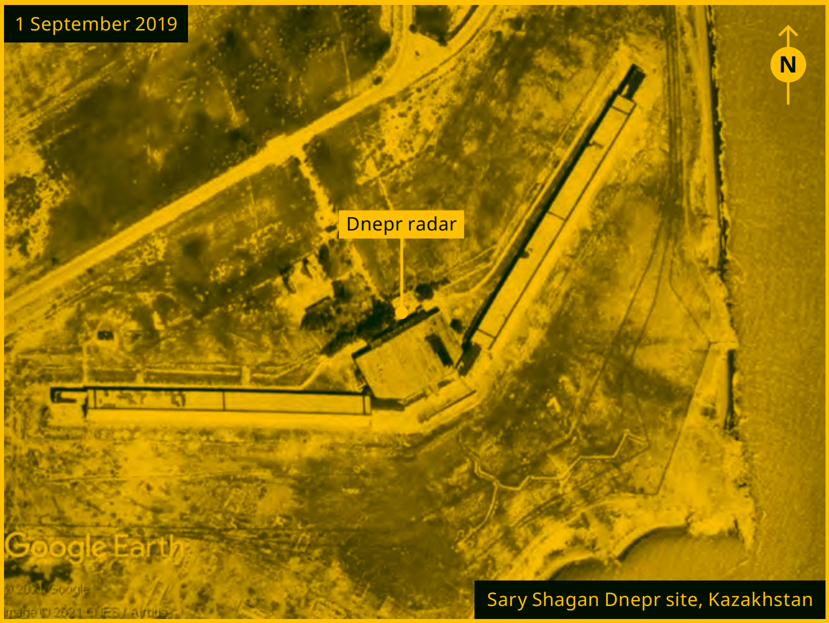
52.874943°N 103.260566°E
(Dnestr)

52.877874°N 103.272584°E
(Dnepr—image shown)

46.603278°N 74.530860°E
(Dnepr—image shown)

68.113720°N 33.910522°E
(Daugava)

FIGURE 16-44 — DNEPR SITE RADAR AT SARY SHAGAN



The image above shows a Dnepr radar array at Sary Shagan.

Function: Radar

Associated Programs: Dnepr/Dnestr

Key Dates: —

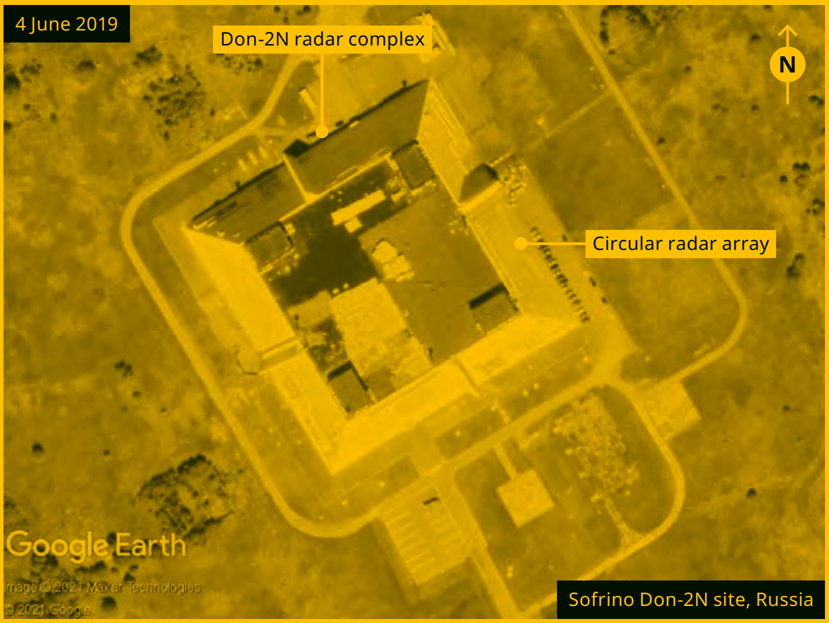
SENSOR COMPLEXES /

RUSSIA >
Radar complexes

56.173299°N 37.769327°E
(Don-2N—image shown)

55.219146°N 37.294505°E
(Dunai-3M)

FIGURE 16-45 — DON-2N SITE AT SOFRINO



The image above shows the Don-2N radar, whose NATO codename is Pill Box, near Sofrino outside of Moscow. It is a critical part of the A-135 ABM system.

Function: Radar

Associated Programs: A-135

Key Dates: —

SENSOR COMPLEXES /

RUSSIA >
Radar complexes

56.173299°N 37.769327°E
(Don-2N)

55.219146°N 37.294505°E
(Dunai-3M—image shown)

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16

FIGURE 16-46 — DUNAI-3M RADAR AT CHEKHOV

The image above shows a Dunai-3M radar at Chekhov, which was part of the A-135 ABM system.

Function: Radar

Associated Programs: A-135

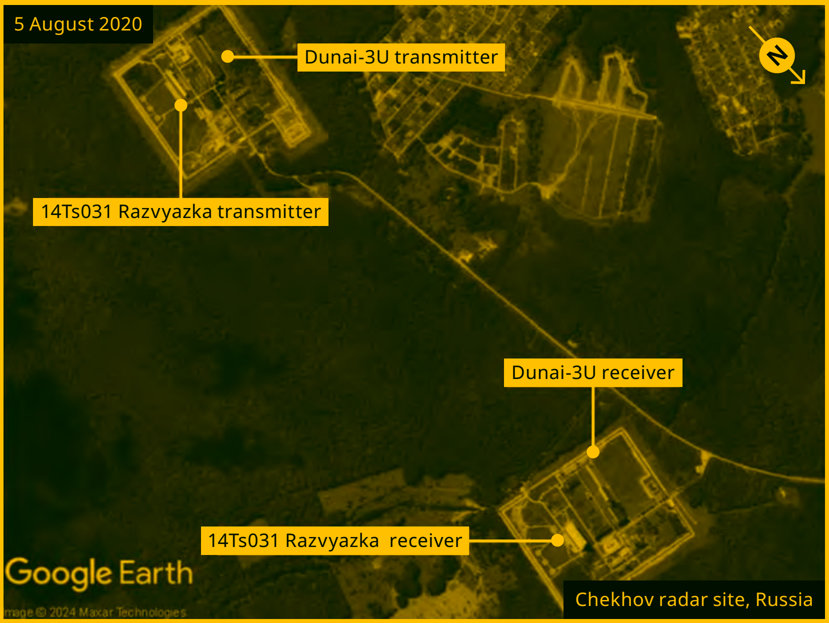
Key Dates: —

RUSSIA >
Radar complexes

55.231292°N 37.298513°E
(Receiver)

55.205850°N 37.295953°E
(Transmitter)

FIGURE 16-47 — RAZVYAZKA RADAR AT CHEKHOV



The image above shows the new Razvyazka radar located near the town of Chekhov southwest of Moscow.

Function: Radar

Associated Programs: —

Key Dates: —

SENSOR COMPLEXES /

RUSSIA >
Radar and optical
telescope complexes

43.826155°N 41.343355°E
(Radar—image shown)

42.935368°N 132.576247°E
(Radar)

43.718100°N 41.227653°E
(30J6 Electro-optical)

FIGURE 16-48 — KRONA RADAR 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. Pictured are the decimeter and centimeter band radar antennas.

Function: Radar

Associated Programs: Krona

Key Dates: —

RUSSIA >
Radar and optical
telescope complexes

43.826155°N 41.343355°E
(Radar)

42.935368°N 132.576247°E
(Radar)

43.718100°N 41.227653°E
(30J6 Electro-optical—image shown)

FIGURE 16-49 — KRONA 30J6 OPTICAL COMPLEX NEAR STOROZHEVAYA

The above image shows the 30J6 component of the Krona complex near Storozhevaya, which contains the optical telescopes and lasers.

Function: Optical telescope

Associated Programs: Krona

Key Dates: —

SENSOR COMPLEXES /

RUSSIA >
Optical telescope complexes

38.280551°N 69.224786°E

FIGURE 16-50 — 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.

Function: Optical telescope complex

Associated Programs: Okno

Key Dates: —

CHINA >
Radar complexes

46.527890°N 130.755269°E
(Huanan)

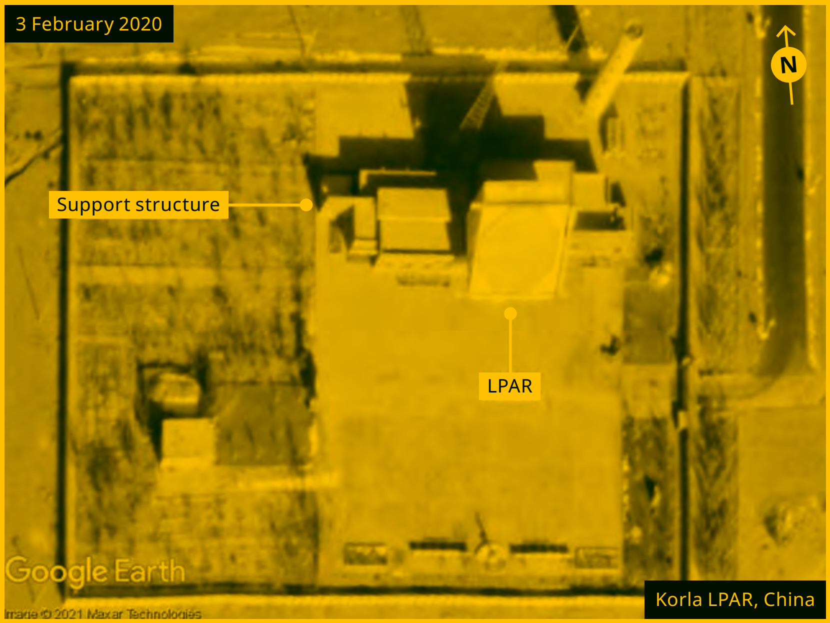
36.024737°N 118.091972°E
(Yiyuan)

30.286623°N 119.128566°E
(Hangzhou)

41.641212°N 86.236834°E
(Korla—image shown)

35.482983°N 106.571819°E
(Kongtong)

FIGURE 16-51 — 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.

Function: Radar

Associated Programs: LPAR

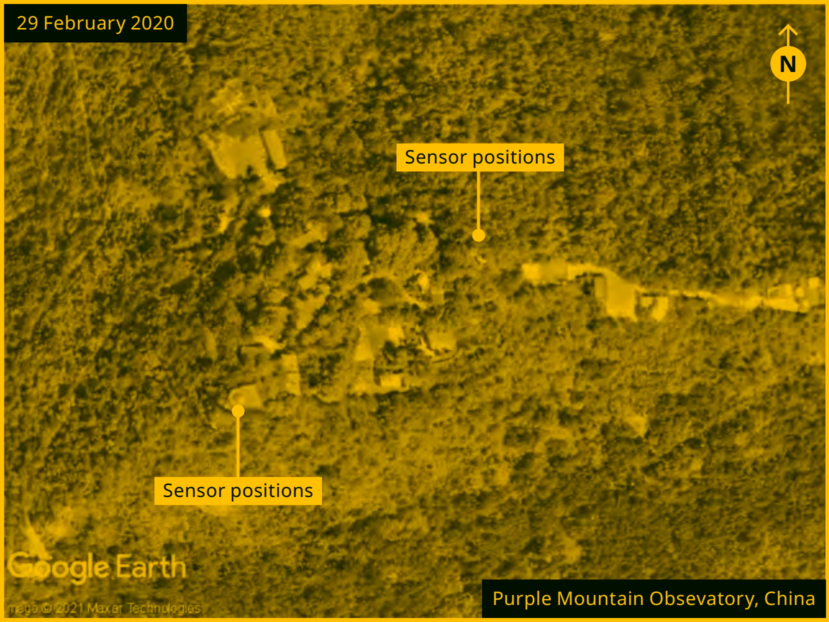
Key Dates: —

SENSOR COMPLEXES /

CHINA >
Optional telescope complexes

32.065°N 118.8297°E

FIGURE 16-52 — 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.

Function: Optical telescope complex

Associated Programs: Purple Mountain Observatory

Key Dates: —

SENSOR COMPLEXES /

FRANCE >
Radar complex

47.3480°N 5.5151°E
(Transmitter—image shown)

44.0715°N 5.5346°E
(Receiver)

FIGURE 16-53 — 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.

Function: Radar

Associated Programs: GRAVES

Key Dates: —

SENSOR COMPLEXES /

FRANCE >
Radar complex

47.3480°N 5.5151°E
(Transmitter)

44.0715°N 5.5346°E
(Receiver—image shown)

FIGURE 16-54 — 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.

Function: Radar

Associated Programs: GRAVES

Key Dates: —

FRANCE >
Optical telescope complex

6.92388889°N 43.75222222°E

FIGURE 16-55 — TAROT-CALERN TELESCOPE

The image above shows the Télescope à Action Rapide pour les Objets Transitoires (Rapid Action Telescope for Transient Objects, TAROT) a pair of 25 centimeters optical telescopes near the Calern Observatory in France that are used to track deep space objects.

Function: Optical telescope complex

Associated Programs: TAROT-CALERN

Key Dates: —

SENSOR COMPLEXES /

INDIA >
Radar complex

19.854052°N 85.969496°E
(Image shown)

13.195549°N 78.173603°E

FIGURE 16-56 — SWORDFISH RADAR NEAR GARHBANGOR

The image above shows the SWORDFISH radar installation near Garhbangor, India.

Function: Radar

Associated Programs: SWORDFISH

Key Dates: —

SENSOR COMPLEXES /

IRAN >
Space surveillance complex

34.119728°N 50.877829°E

FIGURE 16-57 — 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.

Function: Space surveillance complex

Associated Programs:

Key Dates: —

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16

SENSOR COMPLEXES /

JAPAN >
Optical telescope complex

34.672225°N 133.544089°E
(Bisei—image shown)

35.3123°N 133.941364°E
(Kamisaibara)

FIGURE 16-58 — 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.

Function: Optical telescope complex

Associated Programs: Spaceguard

Key Dates: —

SENSOR COMPLEXES /

JAPAN >
Radar complex

34.672225°N 133.544089°E
(Bisei)

35.3123°N 133.941364°E
(Kamisaibara—image shown)

FIGURE 16-59 — KAMISAIBARA SPACEGUARD CENTER

The image above shows the Kamisaibara Spaceguard Center, which is also in Okayama, and is the location of a radar that can track objects in LEO.

Function: Radar

Associated Programs: Spaceguard

Key Dates: —

Design and Art Direction: **ideasbyduchaine.com**

525 Zang Street, Suite D
Broomfield, Colorado 80021
+1 305 554 1560

1779 Massachusetts Ave. NW
Washington, DC 20036
+1 202 568 6212

SWF Publication: 24.04
Published: 24.04

SECURE
WORLD
FOUNDATION

@SWFoundation / info@swfound.org / swfound.org