



COUNTERSPACE CAPABILITIES 101

A 30-INFOGRAPHIC SERIES ON GLOBAL THREATS, TECHNOLOGIES,
DOCTRINES, AND SPACE SECURITY TRENDS

30
INFOGRAPHICS



BASED ON
OPEN-SOURCE
ASSESSMENTS

This series explains the major actors, tools, risks, and strategic dynamics shaping counterspace competition—from destructive anti-satellite weapons and electronic warfare to cyber threats, doctrine, resilience, and emerging trends.

PART I: GLOBAL LANDSCAPE AND CORE THREATS

- 1 GLOBAL COUNTERSPACE CAPABILITIES OVERVIEW
- 2 THE COUNTERSPACE TOOLBOX
- 3 DESTRUCTIVE ANTI-SATELLITE POWERS
- 4 CHINA: CAPABILITIES AND INTENTIONS
- 5 RUSSIA: CAPABILITIES AND INTENTIONS
- 6 EMERGING COUNTERSPACE POWERS
- 7 GPS INTERFERENCE: JAMMING AND SPOOFING
- 8 CYBER THREATS TO SPACE SYSTEMS
- 9 DUAL-USE RPO AND ON-ORBIT SERVICING
- 10 RIPPLE EFFECTS OF SPACE CONFLICT

PART II: DOCTRINE, TECHNOLOGY, AND RESILIENCE

- 11 U.S. COUNTERSPACE POSTURE AND STRATEGY
- 12 SPACE SITUATIONAL AWARENESS AND TRACKING
- 13 ORBITAL DEBRIS FROM ASAT TESTING
- 14 POLICY, DOCTRINE, AND MILITARY ORGANIZATIONS
- 15 DIRECT-ASCENT ASAT WEAPONS
- 16 CO-ORBITAL ASAT SYSTEMS
- 17 DIRECTED-ENERGY WEAPONS
- 18 COMMERCIAL SPACE: VULNERABILITIES AND RISKS
- 19 PROLIFERATED LEO CONSTELLATIONS
- 20 PEACETIME NORMS VS. WARTIME OPERATIONS

PART III: REGIONAL POWERS AND FUTURE TRENDS

- 21 CHINA'S STRATEGY AND SPACE FORCE REORGANIZATION
- 22 RUSSIA'S CO-ORBITAL THREAT AND DOCTRINE
- 23 GPS JAMMING AND SPOOFING HOTSPOTS
- 24 CYBER WARFARE AGAINST SPACE SYSTEMS
- 25 IRAN: COUNTERSPACE CAPABILITIES AND AMBITIONS
- 26 NORTH KOREA'S SPACE AND ASAT ACTIVITIES
- 27 INDIA AFTER MISSION SHAKTI
- 28 EUROPE'S MILITARY SPACE RESPONSE
- 29 THE NUCLEAR ASAT THREAT
- 30 TRENDS SHAPING THE NEXT DECADE



UNDERSTAND THE ACTORS, TOOLS,
AND THREATS IN COUNTERSPACE
COMPETITION.



ENHANCE AWARENESS AND
STRENGTHEN SPACE SECURITY
AND RESILIENCE.



INFORM DECISIONS, POLICY,
AND OPERATIONAL
PLANNING.



ANTICIPATE EMERGING TRENDS
AND PREPARE FOR FUTURE
CHALLENGES.



SUPPORT A STABLE, SECURE,
AND SUSTAINABLE SPACE
ENVIRONMENT.



SERIES THEMES: COUNTERSPACE WEAPONS: • ELECTRONIC WARFARE • CYBER THREATS • SPACE SECURITY • RESILIENCE • NORMS AND DETERRENCE



GLOBAL COUNTERSPACE CAPABILITIES: WHO CAN THREATEN SPACE SYSTEMS?

MODERN COUNTERSPACE CAPABILITIES ARE DESIGNED TO DECEIVE, DISRUPT, DENY, DEGRADE, OR DESTROY SPACE SYSTEMS.

THE COUNTERSPACE LANDSCAPE



States and non-state actors are investing in a broad range of capabilities to challenge space systems across all mission areas.



Capabilities target space systems and the supporting ground segment, links, and data.



These tools can be used in peacetime, crisis, or conflict, often below the threshold of war.



The counterspace ecosystem is expanding rapidly in scale, sophistication, and reach.



Open-source monitoring and transparency are essential for awareness and stability.



COUNTRIES THAT HAVE CONDUCTED DESTRUCTIVE ASAT TESTS

CAPABILITY AREAS	UNITED STATES	RUSSIA	CHINA	INDIA	AUSTRALIA	FRANCE	GERMANY	IRAN	ISRAEL	JAPAN	NORTH KOREA	SOUTH KOREA	UNITED KINGDOM
CO-ORBITAL ASAT Inspect, disrupt, disable, or destroy in space	●	●	●	●	●	●	●	●	●	●	●	●	●
DIRECT-ASCENT ASAT Missiles launched from the Earth's surface	●	●	●	●	—	—	—	—	—	—	—	—	—
ELECTRONIC WARFARE Jamming, spoofing, link deception, signal denial	●	●	●	●	●	●	●	●	●	●	●	●	●
DIRECTED ENERGY Lasers and high-power microwaves	●	●	●	●	●	●	●	●	●	●	●	●	●
CYBER OPERATIONS Attacks on space systems and supporting networks	CYBER COUNTERSPACE CAPABILITIES ARE A GLOBAL ISSUE—NOT LIMITED TO ANY SINGLE COUNTRY. ALL SPACE SYSTEMS AND SUPPORTING NETWORKS ARE POTENTIAL TARGETS FOR MALICIOUS CYBER ACTIVITY.												
SPACE SITUATIONAL AWARENESS (SSA) Track, characterize, and monitor space objects	●	●	●	●	●	●	●	●	●	●	●	●	●
POLICY / ORGANIZATION Doctrine, strategy, units, plans, and partnerships	●	●	●	●	●	●	●	●	●	●	●	●	●

● CAPABILITY FIELDING OR DEVELOPMENT CONFIRMED OR WIDELY REPORTED

● CAPABILITY DEVELOPMENT OR FIELDING REPORTED OR ASSESSED

— NOT INDICATED OR NOT PUBLICLY REPORTED

MAIN CAPABILITY FAMILIES



CO-ORBITAL ASAT
Rendezvous, proximity operations, and on-orbit attacks to disable or destroy satellites.



DIRECT-ASCENT ASAT
Missiles launched from the Earth to intercept and destroy satellites or space objects.



ELECTRONIC WARFARE
Jamming, spoofing, and signal manipulation to disrupt or deny space services.



DIRECTED ENERGY
Lasers and microwave systems to blind, dazzle, disrupt, or damage space systems.



CYBER OPERATIONS
Intrusions and attacks on systems, networks, and data that support space operations.



SPACE SITUATIONAL AWARENESS (SSA)
Sensors, telescopes, and analytics to detect, track, and characterize objects and activities.



POLICY / ORGANIZATION
Strategies, doctrines, organizations, and partnerships that enable counterspace efforts.



WHY IT MATTERS



MILITARY DEPENDENCE: MODERN FORCES RELY ON SPACE FOR COMMUNICATIONS, NAVIGATION, ISR, MISSILE WARNING, AND MORE.



GROWING COMMERCIAL DEPENDENCE: BUSINESSES AND SOCIETIES DEPEND ON SATELLITES FOR CONNECTIVITY, DATA, AND SERVICES.



ESCALATION RISK: COUNTERSPACE ACTIONS CAN TRIGGER CRISES AND ESCALATE CONFLICTS ON EARTH AND IN SPACE.



DEBRIS RISK: DESTRUCTIVE ACTIONS CREATE LONG-LIVED DEBRIS THAT THREATENS ALL SPACE ACTIVITY.



OPEN-SOURCE MONITORING MATTERS: TRANSPARENCY, DATA, AND COLLABORATION HELP REDUCE RISK AND BUILD STABILITY.

THE COUNTERSPACE TOOLBOX: HOW SATELLITES CAN BE DISRUPTED, DISABLED, OR DESTROYED.

FOUR WEAPON FAMILIES. DIFFERENT METHODS. DIFFERENT EFFECTS.

COMPARISON DIMENSIONS	 1. KINETIC WEAPONS USE PHYSICAL FORCE	 2. NON-KINETIC WEAPONS USE RADIATED ENERGY OR RELATED EFFECTS	 3. ELECTRONIC WEAPONS USE ELECTROMAGNETIC SPECTRUM OPERATIONS	 4. CYBER OPERATIONS USE DIGITAL INTRUSION AND MALICIOUS ACTIONS
 ORIGIN OF ATTACK	Primarily from Earth (terrestrial systems). Some attacks from space (e.g., co-orbital).	Primarily from Earth; can also be delivered from the air or space.	From Earth, air, sea, or space platforms and satellites.	From anywhere with network access (Earth-based or in space).
 PERMANENCE OF EFFECT	Typically permanent destruction of the target.	Varies: temporary, reversible, or potentially permanent.	Usually temporary while the system is actively transmitting.	Varies: espionage, disruption (temporary), or permanent disablement/destruction.
 SCALE OF EFFECT	Typically single target, but debris can create cascading effects.	Can be single target or wide-area (e.g., EMP) with collateral impacts.	Can affect one or many systems depending on power, coverage, and techniques.	Can range from single system to enterprise-wide or systemic supply chain impacts.
 ATTRIBUTABILITY	High (launches and debris are typically detectable and traceable).	Moderate to low (effects may be attributed with technical analysis, but can be ambiguous).	Low to moderate (signals may be masked, proxied, or ambiguous).	Low (attackers can hide identity and route; attribution is difficult).
 LAUNCH CAPABILITY REQUIRED	Yes.	No (ground, air, or space delivery may be used).	No.	No.
 SPACE DOMAIN AWARENESS REQUIRED	Yes (to locate, track, and time attacks effectively).	Yes (to target, focus energy, and assess effects).	Yes (to identify emitters, frequencies, and system vulnerabilities).	Yes (to map networks, understand assets, and monitor effects).

 TYPICAL SUBTYPES	 • TERRESTRIAL INFRASTRUCTURE ATTACKS (AGAINST SPACE SYSTEMS ON THE GROUND) • DIRECT-ASCENT ASAT MISSILES • ORBITAL / CO-ORBITAL ASAT ATTACKS	 • DIRECTED ENERGY: LASERS • DIRECTED ENERGY: HIGH-POWER MICROWAVES (HPM) • NUCLEAR DETONATION EFFECTS & EMP (INCLUDED IN SOME TAXONOMIES)	 • JAMMING (DENY, DEGRADE, OR DECEIVE) • SPOOFING (DECEPTION OF SIGNALS AND DATA) • ELECTROMAGNETIC INTERFERENCE	 • TARGETS: GROUND INFRASTRUCTURE, TERMINALS, SPACECRAFT, NETWORKS, AND DATA • EFFECTS: ESPIONAGE, DISRUPTION, OR PERMANENT DISABLEMENT
---	--	---	---	--



SPACE SITUATIONAL AWARENESS (SSA) & INTELLIGENCE: THE ENABLING FUNCTION

Many counterspace operations depend on SSA and intelligence to: locate targets, characterize vulnerabilities, plan operations, and assess results. Strong SSA enables all four weapon families.

KEY TAKEAWAYS

- ✓ COUNTERSPACE CAPABILITIES SPAN KINETIC, NON-KINETIC, ELECTRONIC, AND CYBER TOOLS.
- ✓ EFFECTS RANGE FROM TEMPORARY DISRUPTION TO PERMANENT DESTRUCTION.
- ✓ ATTRIBUTABILITY AND REVERSIBILITY VARY WIDELY BY METHOD.
- ✓ AWARENESS IS THE FOUNDATION: YOU CAN'T TARGET OR DEFEND WHAT YOU CAN'T SEE.
- ✓ RESILIENCE, REDUNDANCY, HARDENING, AND AGILE OPERATIONS REDUCE RISK ACROSS ALL THREATS.

THE FOUR DESTRUCTIVE-ASAT POWERS: UNITED STATES, RUSSIA, CHINA, AND INDIA

THESE ARE THE FOUR COUNTRIES IDENTIFIED IN THE SWF REPORT AS HAVING CONDUCTED DESTRUCTIVE ASAT TESTS.

UNITED STATES		RUSSIA		CHINA		INDIA	
 HISTORICAL TESTING	Conducted both co-orbital (1960s–1970s Program 437) and direct-ascent (1985 ASM-135) destructive ASAT tests.	Soviet Union conducted numerous destructive ASAT tests, including co-orbital systems (e.g., IS series) and direct-ascent tests.		Conducted a destructive direct-ascent ASAT test in 2007 that destroyed a weather satellite.		Conducted a destructive direct-ascent ASAT test, Mission Shakti, in March 2019, intercepting a low Earth orbit satellite.	
 CURRENT BROADER COUNTERSPACE POSTURE	- Includes space control, electronic warfare, cyber operations, offensive counterspace planning, and resilient space architecture. - Invests in non-kinetic and reversible capabilities alongside kinetic options.	- Combines legacy Soviet systems with modern capabilities across: co-orbital, direct-ascent, electronic warfare, and directed-energy development. - Pursues cyber and space situational awareness capabilities.		- Develops a comprehensive counterspace toolkit including: maneuverable and proximity operations satellites, direct-ascent systems, electronic warfare, and cyber capabilities. - Rapidly expanding launch capacity and space infrastructure.		- Continuing to develop military and space-domain capabilities including surveillance, command and control, and indigenous space systems. - Building capabilities across space situational awareness and resilience.	
 NOTABLE CHARACTERISTICS	- Long history of ASAT research and testing. - Leads in space domain awareness, resilient architectures, and allied integration. - In 2022, the United States declared a moratorium on destructive direct-ascent ASAT testing.	- Extensive heritage in ASAT research and operations. - Integrates counterspace options into military doctrine. - Continues to modernize and field counterspace capabilities.		- Pairs history of destructive testing with increasingly advanced and diversified capabilities. - Investing in reusable and rapid-launch systems and resilient architectures. - Focused on deterring and contesting U.S. space advantages.		- Demonstrated direct-ascent ASAT capability in 2019. - Expanding launch capacity and indigenous space technology base. - Emphasizes responsible behavior and a rules-based space order.	

HISTORICAL DESTRUCTIVE ASAT TESTING TIMELINE (SELECTED MILESTONES)

 1960s–1970s UNITED STATES CONDUCTS CO-ORBITAL ASAT TESTS UNDER PROGRAM 437.	 1985 UNITED STATES CONDUCTS DIRECT-ASCENT ASAT TEST (ASM-135) DESTROYING A SOLWIND SATELLITE.	 1968–1982 SOVIET UNION CONDUCTS MULTIPLE CO-ORBITAL AND DIRECT-ASCENT ASAT TESTS.	 2007 CHINA CONDUCTS DIRECT-ASCENT ASAT TEST DESTROYING A WEATHER SATELLITE.	 2019 INDIA CONDUCTS DIRECT-ASCENT ASAT TEST (MISSION SHAKTI) AGAINST A LEO SATELLITE.	 2022 UNITED STATES ANNOUNCES A MORATORIUM ON DESTRUCTIVE DIRECT-ASCENT ASAT TESTING.
---	--	--	--	--	---

THE ORBITAL DEBRIS RISK



DESTRUCTIVE ASAT TESTS CREATE LONG-LIVED DEBRIS THAT CAN DAMAGE OR DESTROY OTHER SATELLITES AND SPACECRAFT, THREATEN CREWED MISSIONS, AND DISRUPT CRITICAL SERVICES RELIED UPON BY ALL COUNTRIES.

THE RISKS DO NOT RESPECT BORDERS—THE DAMAGE IS SHARED BY ALL OPERATORS.

SIMILARITIES AND DIFFERENCES

SIMILARITIES

- ALL FOUR COUNTRIES HAVE CONDUCTED DESTRUCTIVE ASAT TESTS.
- ALL ARE INVESTING IN BROADER COUNTERSPACE CAPABILITIES BEYOND KINETIC WEAPONS.
- ALL VIEW SPACE AS A CRITICAL DOMAIN FOR NATIONAL SECURITY AND DETERRANCE.
- DESTRUCTIVE TESTING CAN GENERATE DEBRIS THAT HARMS EVERYONE.

DIFFERENCES

- THE UNITED STATES HAS HISTORIC CO-ORBITAL AND DA-ASAT PROGRAMS AND HAS DECLARED A DA-ASAT TEST MORATORIUM.
- RUSSIA RELIES ON SOVIET LEGACY WHILE MODERNIZING ACROSS MULTIPLE DOMAINS.
- CHINA COMBINES DESTRUCTIVE TESTING HERITAGE WITH RAPID MODERNIZATION AND EXPANDING LAUNCH CAPACITY.
- INDIA DEMONSTRATED DA-ASAT CAPABILITY IN 2019 AND IS CONTINUING TO DEVELOP.

GLOBAL NORMS AND RESPONSIBLE BEHAVIOR



THE UNITED NATIONS FIRST COMMITTEE ADOPTED A RESOLUTION CALLING ON STATES NOT TO CONDUCT DESTRUCTIVE DIRECT-ASCENT ASAT TESTING. THE RESOLUTION WAS SUPPORTED BY MORE THAN 150 COUNTRIES, REFLECTING STRONG GLOBAL SUPPORT FOR REDUCING ORBITAL DEBRIS RISKS AND PRESERVING THE USE OF OUTER SPACE FOR PEACEFUL PURPOSES.

CHINA'S RAPIDLY EVOLVING COUNTERSPACE CAPABILITIES.

BROADENING TOOLS, IMPROVING PROFICIENCY, AND INCREASING AMBIGUITY.



TOPLINE SUMMARY



THE CSIS REPORT SAYS BEIJING'S RECENT ACTIONS SHOW AN INCREASING EMPHASIS ON THE MILITARY USE OF SPACE.



CHINA CONTINUES TO LAUNCH AND OPERATE HIGHLY MANEUVERABLE DUAL-USE SATELLITES, DEMONSTRATING GROWING OPERATOR PROFICIENCY AND MATURING TACTICS, TECHNIQUES, AND PROCEDURES.



CHINESE ACTIVITIES SPAN CO-ORBITAL CAPABILITIES, DIRECT-ASCENT ASAT, ELECTRONIC WARFARE, DIRECTED ENERGY RESEARCH, CYBER ACTIVITY, AND GROWING SPACE SITUATIONAL AWARENESS.



CHINA HAS ALSO INCREASED LAUNCH ACTIVITY AND MILITARY SPACE ORGANIZATION.



A KEY CONCERN IS THE AMBIGUITY OF DUAL-USE CAPABILITIES: SERVICING, INSPECTION, AND MANEUVERING CAN ALSO SUPPORT COUNTERSPACE OPERATIONS.

CHINA'S COUNTERSPACE CAPABILITIES: A GROWING AND DIVERSIFYING TOOLKIT



CO-ORBITAL CAPABILITIES

Rendezvous, proximity operations, and on-orbit maneuvers that can enable inspection, interference, or attack.



DIRECT-ASCENT ASAT

Missiles launched from the Earth to intercept and destroy satellites or space objects.



ELECTRONIC WARFARE

Jamming, spoofing, and signal manipulation to degrade or deny space services.



DIRECTED ENERGY RESEARCH

Lasers and other directed energy technologies intended to dazzle, degrade, or damage space systems.



CYBER ACTIVITY

Intrusions and attacks on satellite networks, ground systems, and data that support space operations.



SPACE SITUATIONAL AWARENESS

Sensors, telescopes, and analytic capabilities to track, monitor, and characterize objects and activities in space.

MANEUVERABLE SATELLITE FAMILIES OF NOTE



IMPORTANT SPACECRAFT SERIES OFTEN ASSOCIATED WITH ADVANCED MANEUVERS AND RPO ACTIVITY INCLUDE TJS, SJ, AND SY SATELLITES.

TJS

TARGETING AND EXPERIMENTAL SATELLITES

SJ

EXPERIMENTAL AND SERVICING SATELLITES

SY

EXPERIMENTAL TECHNOLOGY SATELLITES

MILESTONES: RECENT EXAMPLES



PRE-2024

MULTIPLE SJ SATELLITES DEMONSTRATE CLOSE PROXIMITY OPERATIONS AND COMPLEX MANEUVERS.

2024

SJ-21 MANEUVERS A DEFUNCT BEIDOU SATELLITE TO GRAVEYARD ORBIT, DEMONSTRATING RPO AND DISPOSAL CAPABILITY.

2025

SJ-25 IS PUBLICLY DESCRIBED AS SUPPORTING FUEL REPLENISHMENT AND LIFE-EXTENSION TESTING; ANALYSTS LINK IT WITH SJ-21.



WHY IT MATTERS



INCREASING RISK

A BROADER AND MORE CAPABLE TOOLKIT RAISES THE RISK TO SATELLITES THAT SUPPORT COMMUNICATIONS, NAVIGATION, ISR, AND ECONOMIC ACTIVITY.



DUAL-USE AMBIGUITY

TECHNOLOGIES THAT ENABLE SERVICING, INSPECTION, AND EXTENSION CAN BE RAPIDLY REPURPOSED TO INTERFERE WITH OR ATTACK OTHER SPACE SYSTEMS.



IMPROVING PROFICIENCY

REPEATED MISSIONS AND MANEUVERS INDICATE GROWING OPERATOR SKILL AND MATURING TACTICS, TECHNIQUES, AND PROCEDURES.



GREATER PERSISTENCE

INCREASED LAUNCH ACTIVITY AND MILITARY SPACE ORGANIZATION ENHANCE CHINA'S ABILITY TO SUSTAIN AND REPLACE CAPABILITIES.



STRATEGIC IMPLICATIONS

COUNTERSPACE CAPABILITIES ENABLE CRISIS COERCION AND ESCALATION CONTROL WHILE COMPLICATING DETERRENCE AND STABILITY IN SPACE.

RUSSIA'S COUNTERSPACE ARSENAL: FROM NUDOL TO ELECTRONIC WARFARE AND NUCLEAR ASAT CONCERNS.

RUSSIA RETAINS A STRONG SOVIET LEGACY AND HAS SPENT THE LAST DECADE REBUILDING OFFENSIVE COUNTERSPACE CAPABILITIES.

RUSSIA'S SIX MAJOR COUNTERSPACE CAPABILITY AREAS

1. CO-ORBITAL ASAT ACTIVITY



- Uses satellites to inspect, approach, and maneuver near other spacecraft.
- Can gather intelligence, interfere with operations, or position for potential future attacks.
- Includes suspicious close-proximity operations in LEO and activity in GEO.

2. DIRECT-ASCENT ASAT DEVELOPMENT



- Develops missiles designed to destroy satellites with a direct hit.
- Nudol (PL-19) is Russia's known direct-ascent ASAT under testing and development.
- Aimed at holding satellites at risk across multiple orbits.

3. ELECTRONIC WARFARE (EW)



- Jamming, spoofing, and deceptive signals to disrupt satellite communications and navigation.
- Long-running pattern of interference in conflict areas and internationally.
- Targets military, commercial, and dual-use systems.

4. DIRECTED ENERGY



- Research and development of lasers and high-power microwave systems to dazzle, degrade, or damage satellites.
- Can be used from the ground, air, or potentially from space.
- Focus on non-kinetic effects that can be reversible—or escalatory.

5. CYBER CAPABILITIES



- Intrusions, malware, and data theft target space systems and networks.
- Can disrupt command and control, corrupt data, or degrade services.
- Blends cyber operations with electronic attacks for greater effect.

6. SPACE SITUATIONAL AWARENESS (SSA)



- Robust tracking, surveillance, and intelligence collection on space objects and operations.
- Supports targeting, deception, and mission planning.
- Includes ground sensors and space-based sensors.



MANYEICES AND COUNTESMENTS (SECURE WORLD FOUNDATION)



EVIDENCE LINKS RUSSIA TO ADVANCED PROGRAMS SUCH AS BUREVESTNIK (NUCLEAR-POWERED CRUISE MISSILE) AND NIVELIR (SPACE-BASED NUCLEAR SYSTEM PROGRAM).



SWF DOCUMENTS A LONG-RUNNING PATTERN OF RUSSIAN JAMMING AND INTERFERENCE AGAINST SATELLITE SYSTEMS IN CONFLICT ZONES AND INTERNATIONALLY.



MAJOR STRATEGIC CONCERN: NUCLEAR ASAT CAPABILITY



RUSSIA IS REPORTED TO BE PURSUING A SPACE-BASED NUCLEAR ASAT CAPABILITY.



IF DEPLOYED OR DETONATED, IT COULD DISRUPT OR DISABLE MANY SATELLITES IN LOW EARTH ORBIT (LEO).



WOULD CREATE MASSIVE AND LONG-LIVED DEBRIS, THREATENING GLOBAL COMMUNICATIONS, NAVIGATION, EARTH OBSERVATION, AND SECURITY.



RAISES SERIOUS TREATY AND ESCALATION CONCERNS, INCLUDING VIOLATIONS OF THE OUTER SPACE TREATY'S PEACEFUL USE PRINCIPLE.



REPRESENTS A WORST-CASE SCENARIO WITH GLOBAL, CIVILIAN, AND MILITARY CONSEQUENCES.



RECENT ACTIVITY HIGHLIGHTS (NOTED BY CSIS)

2020-2023	2021-PRESENT	ONGOING	ONGOING
CLOSE-PROXIMITY MANEUVERS INVOLVING COSMOS 2576, COSMOS 2581, COSMOS 2582, AND COSMOS 2583 IN LOW EARTH ORBIT.	CONTINUED GEO ACTIVITY BY LUCH (OLYMP) SATELLITES, INCLUDING PROXIMITY OPERATIONS.	PATTERN OF JAMMING AND INTERFERENCE AFFECTING SATELLITE SERVICES IN CONFLICT AREAS AND BEYOND.	INTELLIGENCE POINTS TO ADVANCING DIRECT-ASCENT PROGRAMS, INCLUDING NUDOL (PL-19).

WHY RUSSIA'S LAYERED APPROACH MATTERS



MULTI-DOMAIN AND FLEXIBLE
Combines destructive and non-destructive options across multiple domains and orbits.



BELOW THE THRESHOLD
Many actions are non-destructive and reversible, staying below the threshold of armed attack while achieving military effects.



DEGRADE, DISRUPT, DENY
Aims to degrade, disrupt, or deny space services, complicate decision-making, and weaken adversaries.



COMPOUNDING EFFECTS
Layered capabilities can overwhelm defenses and magnify the impact on space-dependent systems.



GLOBAL IMPACT
Threats target all nations' satellites, including commercial and civilian infrastructure.



DETERRENCE CHALLENGE
Dual-use and non-destructive capabilities complicate attribution, response options, and deterrence.

THE EMERGING COUNTERSPACE POWERS: FROM FRANCE AND JAPAN TO IRAN AND NORTH KOREA.

A GROWING NETWORK OF STATES BUILDING COUNTERSPACE CAPABILITIES BEYOND THE PRIMARY DESTRUCTIVE-ASAT GROUP.



AUSTRALIA

- ELECTRONIC WARFARE CAPABILITIES TO DISRUPT SATELLITE SIGNALS.
- ADVANCED SPACE SITUATIONAL AWARENESS (SSA) AS A PRIORITY.
- DEEP ALLIED COOPERATION, ESPECIALLY WITH THE UNITED STATES.



ELECTRONIC WARFARE



SSA



ALLIED COOPERATION



FRANCE

- STRONG INTEREST IN SPACE DEFENSE AND PROTECTIVE MEASURES.
- EXPLORING INSPECTION AND ON-ORBIT VERIFICATION CAPABILITIES.
- INVESTING IN PROTECTIVE SATELLITE CONCEPTS AND RESILIENCE.



SPACE DEFENSE



INSPECTION



PROTECTIVE SATELLITES



GERMANY

- DEVELOPING AN INSPECTOR SATELLITE CONCEPT WITH ROBOTIC ARMS.
- FOCUS ON ON-ORBIT INSPECTION AND OBJECT CHARACTERIZATION.
- BUILDING DUAL-USE TECHNOLOGY AND PARTNERING IN EUROPE.



ROBOTIC INSPECTION



OBJECT CHARACTERIZATION



DUAL-USE TECHNOLOGY



IRAN

- FIELDING MISSILES WITH POTENTIAL ANTI-SATELLITE APPLICATIONS.
- INVESTING IN ELECTRONIC WARFARE AND SIGNAL DISRUPTION.
- GROWING SPACE-SECURITY PROFILE AND CAPABILITY DEVELOPMENT.



MISSILES



ELECTRONIC WARFARE



SPACE SECURITY



ISRAEL

- GPS INTERFERENCE REPORTED IN THE EASTERN MEDITERRANEAN.
- STRONG DIRECTED-ENERGY AND MISSILE-DEFENSE BASE.
- LATENT ASAT POTENTIAL THROUGH DUAL-USE TECHNOLOGIES.



GPS INTERFERENCE



DIRECTED ENERGY



MISSILE DEFENSE



JAPAN

- RAPIDLY INCREASING DEFENSE-SPACE BUDGETS AND CAPABILITIES.
- PRIORITIZING SPACE SITUATIONAL AWARENESS (SSA).
- INTEREST IN PROTECTIVE OR 'BODYGUARD' SATELLITE CONCEPTS.



DEFENSE-SPACE INVESTMENT



SSA



PROTECTIVE SATELLITES



NORTH KOREA

- ACTIVE MISSILE TESTING AND LAUNCH PROGRAMS.
- REPORTED GPS INTERFERENCE AND SIGNAL DISRUPTION.
- ADVANCING SPACE LAUNCH AND SATELLITE CAPABILITIES.



MISSILES



LAUNCH ACTIVITY



GPS INTERFERENCE



SOUTH KOREA

- EXPANDING MILITARY SPACE INVESTMENT AND INFRASTRUCTURE.
- ENHANCING SURVEILLANCE AND RECONNAISSANCE CAPABILITIES.
- BUILDING RESILIENT SPACE ARCHITECTURE AND PARTNERING WITH ALLIES.



SURVEILLANCE



SPACE RESILIENCE



ALLIED COOPERATION



UNITED KINGDOM

- STRONG EMPHASIS ON SPACE DOMAIN AWARENESS (SDA AND SSA).
- INTEGRATING SPACE INTO NATIONAL DEFENSE AND COMMAND STRUCTURES.
- DEEP ALLIED INTEGRATION, ESPECIALLY WITH NATO PARTNERS.



SDA / SSA



DEFENSE INTEGRATION



ALLIED INTEGRATION



INDIA

FAST-RISING REGIONAL POWER

- MISSION SHAKTI (2019) ASAT TEST DEMONSTRATED COUNTERSPACE REACH.
- ADVANCING DOCKING, RPO, AND ON-ORBIT MANEUVER CAPABILITIES.
- RAPIDLY EXPANDING SPACE SITUATIONAL AWARENESS (SSA).



ASAT LEGACY (MISSION SHAKTI)



DOCKING & RPO



SSA EXPANSION

COMMON TRENDS ACROSS EMERGING COUNTERSPACE POWERS



DUAL-USE TECHNOLOGIES

- MANY CAPABILITIES HAVE CIVIL AND MILITARY APPLICATIONS.
- TECHNOLOGY DEVELOPMENT BLURS LINES BETWEEN DEFENSE AND OFFENSE.



SPACE SITUATIONAL AWARENESS GROWTH

- SSA IS A FOUNDATIONAL PRIORITY FOR MOST COUNTRIES.
- IMPROVED DETECTION, TRACKING, AND UNDERSTANDING OF SPACE ACTIVITIES.



ALLIED COOPERATION AND INTEGRATION

- PARTNERSHIPS MULTIPLY ACCESS TO DATA, TECHNOLOGY, AND OPERATIONS.
- INTEGRATION STRENGTHENS DETERRENCE AND RESILIENCE.



ELECTRONIC WARFARE AND SIGNAL DISRUPTION

- GPS INTERFERENCE AND EW CAPABILITIES ARE WIDELY PURSUED.
- LOW-COST, REVERSIBLE TOOLS THAT CAN DEGRADE SPACE SERVICES.

GPS JAMMING AND SPOOFING: THE COUNTERSPACE WEAPON ALREADY AFFECTING DAILY LIFE.

WIDESPREAD. DISRUPTIVE. HARD TO DETECT. DIFFICULT TO ATTRIBUTE.

WHAT'S THE DIFFERENCE?



JAMMING

BLOCKS OR DEGRADES THE SIGNAL.

Jamming overwhelms satellite signals with noise or interference, preventing receivers from getting accurate position, navigation, and timing (PNT) data.



SPOOFING

TRICKS A RECEIVER WITH A FALSE SIGNAL.

Spoofing transmits fake satellite signals that appear legitimate, deceiving receivers into calculating the wrong position, speed, or time without losing signal lock.



CSIS FINDINGS

The CSIS report identifies widespread GPS interference around conflict zones and flashpoints, including the Baltic and Nordic region, Ukraine and Russia, the eastern Mediterranean and Middle East, the Korean Peninsula, and South Asia.

NOTABLE INCIDENTS: 2024-2025

1 MAY 2024



FINNAIR CANCELLED FLIGHTS TO TARTU, ESTONIA, DUE TO GPS INTERFERENCE AFFECTING SAFETY.

2 LATE MAY – EARLY JUNE 2024



NORTH KOREAN INTERFERENCE AFFECTED ROUGHLY 500 PLANES AND HUNDREDS OF SHIPS IN THE REGION.

3 LATE 2024



RISE IN GPS INTERFERENCE INCIDENTS REPORTED IN JORDAN IMPACTING AVIATION AND OTHER USERS.

4 JANUARY 2025



RYANAIR FLIGHT DIVERTED NEAR NATO'S EASTERN BORDER DUE TO GPS INTERFERENCE.

5 2023-2024



IATA REPORTED A 500 PERCENT INCREASE IN GPS SPOOFING INCIDENTS BETWEEN 2023 AND 2024.



THE CSIS REPORT NOTES THAT RUSSIA, NORTH KOREA, AND ISRAEL WERE WIDELY ASSOCIATED WITH MAJOR INTERFERENCE PATTERNS DISCUSSED IN THE STUDY PERIOD.

WHO IS AFFECTED? REAL-WORLD IMPACTS ACROSS CIVIL AND MILITARY USERS



AVIATION

Disrupted navigation, flight diversions, delays, cancellations, and increased pilot workload and risk.



SHIPPING

Loss of position accuracy, route deviations, port delays, and higher risk of collisions and groundings.



EMERGENCY RESPONSE

Interference can delay or misdirect emergency services and reduce situational awareness.



TIMING SERVICES

Disrupts precise time needed for telecom, power grids, finance, broadcast, and other critical infrastructure.



EVERYDAY NAVIGATION

Impacts maps, ride-hailing, delivery, agriculture, surveying, and personal navigation applications.



THE BOTTOM LINE: A COUNTERSPACE WEAPON WITH EVERYDAY CONSEQUENCES

GPS JAMMING AND SPOOFING ARE REAL, RISING, AND ROUTINELY IMPACTING CIVIL LIFE. DIPLOMATIC CONDEMNATION HAS NOT ELIMINATED THE PRACTICE.

CYBER WARFARE AGAINST SPACE SYSTEMS: THE LOW-VISIBILITY COUNTERSPACE THREAT.

HIDDEN IN NETWORKS. HARD TO ATTRIBUTE. DESIGNED TO STEAL, DISRUPT, DENY, DEGRADE, OR DESTROY SPACE CAPABILITIES.

ATTACK SURFACE: WHERE CYBER OPERATIONS CAN STRIKE

CYBER COUNTERSPACE OPERATIONS CAN TARGET MULTIPLE ELEMENTS ACROSS THE SPACE ECOSYSTEM.

SPACECRAFT	ONBOARD SYSTEMS, PAYLOADS, FLIGHT SOFTWARE, TELEMETRY, AND COMMAND LINKS.
GROUND STATIONS	TELECOMMAND, TELEMETRY, TRACKING, AND MISSION CONTROL SYSTEMS.
SATELLITE TERMINALS	USER TERMINALS, IOT DEVICES, AND ASSOCIATED GATEWAYS.
NETWORKS	ENTERPRISE IT, MISSION NETWORKS, DATA LINKS, AND CLOUD ENVIRONMENTS.
MISSION SYSTEMS	PLANNING, TASKING, DATA PROCESSING, ANALYTICS, AND CONTROL APPLICATIONS.
SPACEPORTS	LAUNCH SYSTEMS, RANGE OPERATIONS, GROUND SUPPORT, AND LOGISTICS.
SUPPORTING INFRASTRUCTURE	POWER, FACILITIES, SUPPLY CHAIN, THIRD-PARTY PROVIDERS, AND SHARED SERVICES.

ATTACK TYPES AND EFFECTS

CYBER OPERATIONS CAN BE TAILORED TO ACHIEVE A RANGE OF OUTCOMES AGAINST SPACE SYSTEMS AND SUPPORTING INFRASTRUCTURE.

ESPIONAGE	UNAUTHORIZED ACCESS TO SYSTEMS AND DATA FOR INTELLIGENCE GATHERING AND SITUATIONAL AWARENESS.
DATA THEFT	EXFILTRATION OF SENSITIVE DATA, INTELLECTUAL PROPERTY, AND OPERATIONAL INFORMATION.
DISRUPTION	INTERFERENCE WITH SYSTEMS OR PROCESSES CAUSING DEGRADATION, ERRORS, OR TIMING DELAYS.
SERVICE DENIAL	DENYING ACCESS TO SERVICES OR NETWORKS THROUGH OVERLOADS, BLOCKING, OR RESOURCE EXHAUSTION.
RANSOMWARE	MALICIOUS ENCRYPTION OR LOCKOUT TO EXTRACT PAYMENT OR COERCE ACTION.
MANIPULATION	ALTERING DATA, COMMANDS, OR CONFIGURATIONS TO DECEIVE, MISDIRECT, OR SUBVERT OPERATIONS.
PERMANENT DISABLEMENT	DESTROYING, CORRUPTING, OR BRICKING SYSTEMS TO CAUSE LONG-TERM OR IRREVERSIBLE LOSS.

WHY THIS THREAT IS HARD TO SEE AND STOP

CYBER OPERATIONS LEVERAGE AMBIGUITY, STEALTH, AND COMPLEXITY TO OPERATE BELOW THE THRESHOLD OF DETECTION AND RESPONSE.

AMBIGUITY	ATTACKERS' INTENT IS OFTEN UNCLEAR. THE SAME ACTIVITIES CAN APPEAR TO BE ROUTINE OR ACCIDENTAL.
ATTRIBUTION CHALLENGES	ATTACKS ARE ROUTED THROUGH PROXIES, STOLEN ACCOUNTS, AND GLOBAL INFRASTRUCTURE, MAKING ATTRIBUTION SLOW, UNCERTAIN, AND CONTESTED.
TARGET UNCERTAINTY	DETERMINING WHETHER A GIVEN INCIDENT TRULY TARGETED SPACE SYSTEMS CAN BE DIFFICULT AND TIME-CONSUMING.
STEALTH AND PERSISTENCE	ADVERSARIES USE LIVING-OFF-THE-LAND TECHNIQUES, ENCRYPTION, AND SLOW OPERATIONS TO AVOID DETECTION.
SLOW-BURN IMPACT	EFFECTS MAY APPEAR DAYS, WEEKS, OR MONTHS AFTER INITIAL ACCESS, COMPLICATING RESPONSE AND RECOVERY.
WIDENING ATTACK SURFACE	COMPLEX SUPPLY CHAINS, LEGACY SYSTEMS, AND THIRD-PARTY ACCESS INCREASE EXPOSURE AND RISK.



A PERSISTENT AND GROWING PROBLEM

THE SPACE SECTOR HAS SEEN A STEADY STREAM OF CYBER INCIDENTS IMPACTING GOVERNMENT, CRITICAL INFRASTRUCTURE, AND COMMERCIAL ENTITIES ACROSS THE GLOBE.



LOWER BARRIER THAN KINETIC WEAPONS—BUT NOT TRIVIAL

CYBER CAPABILITIES CAN HAVE A MUCH LOWER BARRIER TO ENTRY THAN KINETIC COUNTERSPACE WEAPONS, ENABLING MORE ACTORS. ADVANCED OPERATIONS STILL REQUIRE SKILL, ACCESS, AND RESOURCES.

HOW TO REDUCE RISK

1 SEGMENT AND ISOLATE SEGMENT NETWORKS BY MISSION AND CRITICALITY. ISOLATE ESSENTIAL SYSTEMS FROM UNNECESSARY ACCESS AND UNTRUSTED NETWORKS.	2 ENCRYPT EVERYWHERE USE STRONG ENCRYPTION FOR DATA AT REST, IN TRANSIT, AND IN USE. PROTECT CREDENTIALS, KEYS, AND SENSITIVE INFORMATION.	3 PATCH AND HARDEN KEEP SYSTEMS, FIRMWARE, AND SOFTWARE UP TO DATE. REMOVE UNNECESSARY SERVICES AND DEFAULT ACCOUNTS. APPLY SECURE CONFIGURATIONS.	4 MONITOR AND DETECT IMPLEMENT CONTINUOUS MONITORING, LOGGING, AND ANOMALY DETECTION ACROSS IT, OT, AND MISSION ENVIRONMENTS.	5 SHARE AND COLLABORATE PARTICIPATE IN INCIDENT SHARING AND THREAT INTELLIGENCE COMMUNITIES TO IMPROVE AWARENESS AND RESPONSE.	6 PLAN AND PRACTICE DEVELOP INCIDENT RESPONSE AND RECOVERY PLANS. TEST THROUGH TABLETOPS AND EXERCISES.	7 IMPROVE CYBER HYGIENE ENFORCE STRONG ACCESS CONTROLS, MFA, LEAST PRIVILEGE, TRAIN USERS, AND VET SUPPLIERS THROUGHOUT THE SUPPLY CHAIN.
--	--	--	---	--	---	---

FRIENDLY SATELLITE OR SPACE WEAPON? THE DUAL-USE PROBLEM OF RPO, SERVICING, AND ROBOTICS.

THE SAME TECHNOLOGIES THAT ENABLE PEACEFUL OPERATIONS CAN ALSO SUPPORT COUNTERSPACE MISSIONS.

PEACEFUL USES

SUPPORTING SPACE SAFETY, SUSTAINABILITY, AND VALUE



INSPECTION & HEALTH CHECKS

Assess satellite condition to ensure safety and extend mission reliability.



SERVICING & REPAIR

Replace or fix components to keep satellites operational and reduce space debris.



REFUELING

Extend spacecraft life by replenishing propellant supplies.



DOCKING & BERTHING

Enable spacecraft to connect for crew, cargo, or technology transfer.



DEBRIS REMOVAL

Capture and remove defunct objects to improve long-term space sustainability.



LIFE EXTENSION

Add years of service to valuable satellites, protecting economic and societal benefits.

HOW AMBIGUITY ARISES

THE SAME CAPABILITIES CAN MEAN DIFFERENT THINGS

1. CAPABILITY DEVELOPED



Robotic arms, sensors, propulsion, and autonomy enable close-approach and interaction.

2. CLOSE APPROACH



Rendezvous and proximity operations (RPO) bring objects within inspection or interaction range.

3. OBSERVED BEHAVIOR



Maneuvers, station-keeping, arm deployment, or contact look similar from the outside.

4. UNKNOWN INTENT



Observers cannot know purpose: service, experiment, commercial activity, or something else.

5. DIFFERENT INTERPRETATIONS



The same behavior may be seen as defensive, commercial, experimental, or threatening—depending on context.



THE CENTRAL CHALLENGE: AMBIGUITY OF INTENT

Without clear information, close approaches and on-orbit interactions can be misread, creating risk of misunderstanding, escalation, or countermeasures.

POTENTIAL MILITARY USES

CAPABILITIES THAT CAN SUPPORT COUNTERSPACE MISSIONS



SURVEILLANCE & INTELLIGENCE

Inspect and characterize other satellites for targeting and intelligence.



INTERFERENCE & DISABLEMENT

Jam, dazzle, spoof, or physically disrupt sensors and communications.



CAPTURE & CONTROL

Grapple or seize satellites to move, reposition, or deorbit them.



REFUELING FOR OFFENSIVE MISSIONS

Extend the life or reach of satellites used for hostile operations.



DIRECT-ASAT ATTACKS

Damage, destroy, or deorbit satellites kinetically or non-kinetically.



REPOSITIONING & DEORBITING

Move satellites from their orbits or force them to reenter.

EVIDENCE HIGHLIGHTED IN REPORTS AND PUBLIC SOURCES



RPO DEFINITION

RPO stands for rendezvous and proximity operations.

It includes activities where spacecraft purposefully approach, operate near, or interact with another space object.



DUAL-USE CONCERNS

Reports highlight dual-use concerns around:

- Maneuverable satellites
- Robotic arms
- Grapplers and capture tools
- Close-approach operations

These capabilities enable both beneficial and harmful uses.



CHINA'S PROGRAMS

China's SJ-21 satellite in 2022 moved a defunct satellite to graveyard orbit.

SJ-25 has been presented as supporting refueling or life-extension technology testing.



COMMERCIAL & CIVIL EXAMPLES

Companies and agencies are developing in-space servicing and debris-removal concepts, including:

- Robotic servicing and repair
- Nets and harpoons
- Other capture and containment tools
- Docking and life-extension systems

These advance sustainability and reduce debris.



RUSSIA & CHINA CONCERNS

Russia's Luch ("Olymp-K") satellites and multiple Chinese satellite families (e.g., SJ series, Shijian series, and others) have demonstrated proximity capabilities.

These activities contribute to broader concern about how intent is interpreted.



OBSERVER DILEMMA

Observers must judge intent with limited data.

The same maneuver can be seen as maintenance today and a threat tomorrow depending on context, history, and information available.

WHY NORMS, TRANSPARENCY, AND SSA MATTER



TRANSPARENCY

Sharing mission intent, capabilities, and operational constraints builds confidence and reduces suspicion.



NOTIFICATION

Advance or timely notice of planned RPO and close approaches helps others prepare and interpret actions.



NORMS OF BEHAVIOR

Agreed principles—such as safe operating distances and responsible RPO—reduce risk of escalation.



SPACE SITUATIONAL AWARENESS (SSA)

Better tracking, data sharing, and information fusion improve common awareness and interpretation.



REDUCING ESCALATION

Clear information and shared norms help prevent miscalculation and maintain a stable space environment.



THE GOAL IS NOT TO LIMIT PEACEFUL INNOVATION—BUT TO MANAGE RISK AND PRESERVE STABILITY IN SPACE. RESPONSIBLE USE, CLEAR COMMUNICATION, AND INTERNATIONAL COOPERATION ARE ESSENTIAL.

WHY SPACE CONFLICT COULD SPREAD FAR BEYOND THE SATELLITES: DEBRIS, COMMERCIAL TARGETS, AND ESCALATION

WHAT HAPPENS IN SPACE CAN RIPPLE INTO AVIATION, SHIPPING, EMERGENCY SERVICES, FINANCIAL TIMING, COMMUNICATIONS, AND DAILY LIFE ON EARTH.



COUNTERSPACE CONFLICT CAN AFFECT FAR MORE THAN SATELLITES: IT CAN DISRUPT COMMUNICATIONS, NAVIGATION, ISR, MISSILE WARNING, TIMING, AND COMMERCIAL SERVICES USED ON EARTH.

1. ORBITAL EVENT



DESTRUCTIVE ATTACKS

Kinetic, directed energy, or electronic attacks on spacecraft.



ACCIDENTAL BREAKUPS

Collisions, explosions, or anomalies create debris.



NON-KINETIC EFFECTS

Jamming, spoofing, dazzling, or cyber operations degrade or disable systems.



MISATTRIBUTION & AMBIGUITY

Limited information and dual-use capabilities create uncertainty and escalate crises.

2. SPACE EFFECTS



DEBRIS GENERATION

Destructive attacks and accidental breakups create debris that can threaten other spacecraft and increase long-term risk.



LOSS OR DEGRADATION OF SPACE SYSTEMS

Satellites for communications, navigation, ISR, missile warning, and timing can be degraded, denied, or destroyed.



CONSTELLATION VULNERABILITIES

Large proliferated constellations improve resilience, but they also introduce new strategic questions about how they might be targeted or defended.



ESCALATION DYNAMICS

Ambiguity, misattribution, and the dual-use nature of space systems can accelerate escalation and broaden conflict.

3. EARTH EFFECTS



COMMUNICATIONS

Disrupted voice, data, broadcast, and internet services.



NAVIGATION & TIMING

Loss of GPS/GNSS impacts transport, logistics, precision operations, and financial timing.



ISR & DOMAIN AWARENESS

Reduced ability to detect threats, monitor crises, and inform decision-making.



MISSILE WARNING

Degraded detection and tracking increase risk of miscalculation.



COMMERCIAL & ECONOMIC IMPACTS

Disrupted services for aviation, shipping, energy, emergency services, agriculture, and finance.



PUBLIC SAFETY & DAILY LIFE

Emergency response, safety-of-life services, and everyday activities are affected.

DEBRIS CASE STUDY: UNINTENTIONAL GENERATION



- THE CSIS REPORT ADDED A SPECIAL DISCUSSION ON UNINTENTIONAL DEBRIS GENERATION.
- IT HIGHLIGHTS INCIDENTS SUCH AS THE LONG MARCH 6A UPPER-STAGE BREAKUP IN AUGUST 2024.
- THIS EVENT CREATED SEVERAL HUNDRED TRACKABLE FRAGMENTS AND POSSIBLY MANY MORE.
- UNINTENTIONAL EVENTS CAN POSE RISKS COMPARABLE TO DELIBERATE ATTACKS.

COMMERCIAL ENTANGLEMENT



- COMMERCIAL OPERATORS ARE INCREASINGLY ENTANGLED WITH NATIONAL SECURITY.
- CIVILIAN SATELLITES AND SERVICES SUPPORT CRITICAL GOVERNMENT AND MILITARY MISSIONS.
- THIS MAKES COMMERCIAL SYSTEMS POTENTIAL TARGETS OR SOURCES OF ESCALATION.
- DISRUPTION CAN HARM ECONOMIES AND POPULATIONS WITHOUT DIRECT MILITARY ENGAGEMENT ON EARTH.

KEY TAKEAWAY



- SPACE CONFLICT CAN SPREAD FAR BEYOND THE SATELLITES.
- DEBRIS, DISRUPTION, AND UNCERTAINTY CAN IMPACT CRITICAL SERVICES AND DAILY LIFE.
- THE COSTS WILL BE GLOBAL, NOT LIMITED TO THE INITIAL TARGET.
- STABILITY IN SPACE IS ESSENTIAL FOR A STABLE AND RESILIENT WORLD.

WHY RESTRAINT AND TRANSPARENCY MATTER



REDUCE RISKS OF MISPERCEPTION AND ESCALATION.



SHARE INFORMATION ON OPERATIONS AND INCIDENTS, INCLUDING DEBRIS EVENTS.



ADOPT NORMS OF RESPONSIBLE BEHAVIOUR AND DEBRIS MITIGATION.



STRENGTHEN COOPERATION ACROSS GOVERNMENTS AND INDUSTRY.



BUILD RESILIENCE AND PREPARE FOR DISRUPTION TO PROTECT PEOPLE ON EARTH.

UNITED STATES COUNTERSPACE POSTURE: FROM SPACE SUPERIORITY TO CONTESTED SPACE



THE UNITED STATES HAS THE MOST ADVANCED MILITARY SPACE CAPABILITIES, BUT THE RELATIVE GAP WITH CHINA IS NARROWING.



THE UNITED STATES PIONEERED MANY MILITARY SPACE APPLICATIONS AND HAS EXTENSIVE OPERATIONAL EXPERIENCE INTEGRATING SPACE INTO JOINT OPERATIONS.



THE UNITED STATES FIELDS ACKNOWLEDGED ELECTRONIC-WARFARE COUNTERSPACE SYSTEMS AND IS DEVELOPING ADDITIONAL OFFENSIVE COUNTERSPACE CAPABILITIES.



U.S. FOCUS NOW INCLUDES RESILIENCE, SPACE CONTROL, CONTESTED-SPACE OPERATIONS, AND INTEGRATION ACROSS THE JOINT FORCE.



MAJOR ORGANIZATIONAL CHANGES INCLUDE THE CREATION OF THE U.S. SPACE FORCE (2019) AND U.S. SPACE COMMAND (2019). IN 2022, THE UNITED STATES ANNOUNCED A MORATORIUM ON DESTRUCTIVE DIRECT-ASCENT ASAT TESTING.

CAPABILITY AREAS



CO-ORBITAL TECHNOLOGY BASE

- The United States has demonstrated co-orbital inspection and proximity operations technologies.
- These capabilities provide options for denying, disrupting, or degrading adversary space systems.



DIRECT-ASCENT ASAT LEGACY

- The United States developed direct-ascent ASAT missiles during the Cold War.
- Tests in the 1980s validated the capability; the United States has not conducted destructive DA-ASAT testing since 2008.



ELECTRONIC WARFARE

- The United States fields electronic-attack systems that can jam, spoof, or degrade adversary space systems and links.
- EW is a core counterspace capability used to create effects without physical attack.



DIRECTED ENERGY RESEARCH

- The United States is investing in directed energy technologies for potential future use against space targets.
- Efforts focus on maturing lasers, power, and control systems for scalability and resilience.



SPACE SITUATIONAL AWARENESS

- The United States operates the world's most capable space surveillance network.
- SSA enables tracking, characterization, and warning to protect U.S. and allied space assets.



CYBER / RESILIENCE

- Cyber operations can target space systems and supporting ground systems.
- Resilience includes proliferated architectures, hardening, rapid reconstitution, and protected control.



POLICY / DOCTRINE

- U.S. doctrine emphasizes deterrence, proportional response, and responsible behavior in space.
- The United States seeks to hold adversaries at risk while avoiding destabilizing space arms races.

ORGANIZATION AND STRATEGY



U.S. SPACE FORCE

- Established December 20, 2019 as the sixth branch of the U.S. Armed Forces.
- Responsible for organizing, training, and equipping space forces; developing space professionals; and presenting forces to combatant commanders.



U.S. SPACE COMMAND

- Established August 29, 2019 as a unified combatant command.
- Plans, integrates, and conducts military operations in, from, and to space to deter aggression and, if necessary, defeat adversary threats.



ALLIED INTEGRATION

- The United States works closely with allies and partners to share data, synchronize operations, and build combined space capabilities.
- Coalitions strengthen deterrence and improve resilience in contested space.



CONTESTED-SPACE READINESS

- Strategy emphasizes space control, contested-space operations, and rapid adaptation.
- Integration across the joint force ensures space capabilities are employed in support of all-domain operations.

SELECTED MILESTONES



1960s-1980s COLD WAR ASAT EFFORTS

The United States develops and tests direct-ascent ASAT missiles.



1985
ASM-135 ASAT TEST
U.S. successfully tests the ASM-135 against a target satellite.



2008 LAST DESTRUCTIVE DA-ASAT TEST

The United States does not conduct destructive DA-ASAT testing since 2008.



2019 U.S. SPACE FORCE ESTABLISHED

The Space Force is established as a new military service on December 20, 2019.



2019 U.S. SPACE COMMAND ESTABLISHED

USSPACECOM is established on August 29, 2019.



2022 DA-ASAT TEST MORATORIUM

The United States announces a moratorium on destructive direct-ascent ASAT testing.

WHY IT MATTERS / KEY TAKEAWAYS



MODERN MILITARY OPERATIONS DEPEND ON SPACE FOR SECURE COMMUNICATIONS, NAVIGATION, INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE (ISR), AND MISSILE WARNING.



ADVERSARIES ARE INVESTING IN CAPABILITIES TO CONTEST, DISRUPT, OR DESTROY U.S. SPACE SYSTEMS.



A COMPREHENSIVE U.S. COUNTERSPACE POSTURE—COMBINING OFFENSE, DEFENSE, RESILIENCE, AND ALLIANCE—PRESERVES FREEDOM OF ACTION AND DETERRENCE.



THE UNITED STATES REMAINS COMMITTED TO RESPONSIBLE BEHAVIOR IN SPACE AND TO A STABLE, SUSTAINABLE SPACE ENVIRONMENT.

SPACE SITUATIONAL AWARENESS:

THE FOUNDATION OF COUNTERSPACE OPERATIONS



SPACE SITUATIONAL AWARENESS (SSA)

is the ability to detect, track, characterize, and understand space objects and the environment.



WHERE OBJECTS
ARE



WHAT THEY ARE
DOING



HOW THEY ARE
BEHAVING



WHETHER BEHAVIOR IS
ROUTINE OR SUSPICIOUS



WHAT RISKS THEY
MAY POSE

MANY SPACE ATTACKS AND DEFENSIVE ACTIONS DEPEND ON KNOWING:

CORE FUNCTIONS OF SSA



DETECT

Sense objects and events in space.



TRACK

Determine and maintain precise orbits and trajectories.



IDENTIFY

Determine what an object is and its ownership when possible.



CHARACTERIZE

Assess size, shape, purpose, capabilities, and intent.



PREDICT

Forecast future positions and behaviors to anticipate risk.

KEY ASSETS ENABLING SSA



GROUND RADARS

Detect and track objects in LEO, GEO, and GEO, day or night, through weather.



OPTICAL TELESCOPES

Provide high-precision tracking and characterization of satellites and objects.



SPACE-BASED SENSORS

Extend coverage, reduce blind zones, and provide early warning from advantageous vantage.



DATA FUSION & ANALYTICS

Combine data from many sources to create a common operational picture and detect anomalies.



INFORMATION SHARING

Timely exchange of data and alerts strengthens collective awareness and coordination.

WHY SSA MATTERS FOR COUNTERSPACE OPERATIONS & DEFENSE



COLLISION AVOIDANCE

Protects satellites, spacecraft, and people by avoiding debris and close approaches.



EARLY WARNING

Detects potential threats and hostile actions early to enable timely response.



ATTRIBUTION SUPPORT

Provides evidence and context to support attribution of malicious activity.



MISSION ASSURANCE

Enables resilient planning and operations through understanding of the space domain.



PROTECTS ALL USERS

Safeguards military, civil, and commercial space systems and the services they provide.

CHALLENGES TO EFFECTIVE SSA



CROWDING & DEBRIS

More objects and debris increase risk and complicate tracking.



DUAL-USE ACTIVITY

Many capabilities have both benign and malicious potential, blurring intent.



DATA GAPS

Sensor limitations, coverage gaps, and weather reduce visibility.



AMBIGUITY

Limited information can make behavior difficult to interpret with confidence.



ATTRIBUTION LIMITS

Technical and political complexities can make attribution slow and challenging.

KEY TAKEAWAYS



SSA is the foundation for understanding the space environment and acting with confidence.



It enables timely decisions, reduces risk, and strengthens deterrence and response.



Investment in sensors, analytics, and sharing multiplies awareness and effectiveness.



A comprehensive, persistent, and resilient SSA architecture is essential for safety and security.



Better SSA improves both safety and security in space.

ORBITAL DEBRIS FROM DESTRUCTIVE ASAT TESTING: THE DAMAGE THAT OUTLIVES THE ATTACK



DESTRUCTIVE ANTI-SATELLITE (ASAT) TESTS SHATTER TARGETS.

Explosions or high-speed collisions create thousands of fast-moving fragments.



DEBRIS REMAINS IN ORBIT FOR YEARS OR DECADES.

Fragments can stay in space long after the test and continue to pose collision risks.



OTHERS PAY THE PRICE.

Debris endangers satellites operated by many nations for communication, navigation, science, and security.



A SHARED ENVIRONMENT REQUIRES SHARED RESPONSIBILITY.

Reducing debris protects space activities and benefits all nations and peoples.

DESTRUCTIVE DIRECT-ASCENT ASAT TESTS: A HISTORY OF LASTING CONSEQUENCES



UNITED STATES

1985

SM-3 ASAT TEST

Solwind P78-1 satellite

- Intercepted at high altitude.
- Created many tracked debris pieces that remain in orbit today.
- Demonstrated capability—but left a debris legacy.



SOVIET UNION / RUSSIA

1968, 1982, 1985

MULTIPLE ASAT TESTS

Co-orbital and direct-ascent

- Many tests against satellites in low Earth orbit.
- Produced long-lived debris fields.
- Legacy debris continues to pose collision risks.



CHINA

2007

SC-19 ASAT TEST

FY-1C weather satellite

- Intercepted at low Earth orbit.
- Generated thousands of debris pieces.
- One of the largest single debris-creating events in history.



INDIA

2019

MISSION SHAKTI ASAT TEST

Microsat-R satellite

- Intercepted in low Earth orbit.
- Created debris that remains a risk to space operations.
- Demonstrated capability with lasting consequences.



EVERY DESTRUCTIVE ASAT TEST HAS CREATED DEBRIS.

These fragments travel at orbital speeds and remain a hazard long after the test is over.

WHY DEBRIS MATTERS



COLLISION RISK

Debris moves at kilometers per second. Even small fragments can disable or destroy satellites.



PERSISTENCE

Fragments can remain in orbit for years or decades, especially in low Earth orbit (LEO).



DIFFICULT TO CLEAN UP

Most debris is too small to track or capture. Active removal is complex, costly, and still emerging.



THREATS TO ALL USERS

Civil, commercial, and military satellites share the same orbital environment. Debris does not respect borders.

DEBRIS SOURCES

MULTIPLE ACTIVITIES ADD TO THE PROBLEM



DESTRUCTIVE ASAT TESTS

Deliberate tests that intentionally destroy a satellite using a missile or other kinetic means. These events create large numbers of trackable debris pieces.



ACCIDENTAL BREAKUPS

Explosions from leftover fuel, battery failures, or thermal events can fragment satellites or upper stages.



OTHER FRAGMENTATION

Collisions between objects and impacts from micrometeoroids or small debris also create additional fragments.

WHY RESPONSIBLE BEHAVIOR MATTERS



PROTECTS THE SPACE ENVIRONMENT

Limiting debris-generating activities reduces current risks and preserves long-term access to space.



SUPPORTS STABILITY AND TRUST

Responsible actions lower the risk of misunderstanding, escalation, and an arms race in space.



ENABLES GLOBAL BENEFITS

Satellites support communications, navigation, disaster response, climate monitoring, and economies worldwide.



A PRACTICAL, VERIFIABLE COMMITMENT

Norms and transparency measures build confidence and reinforce responsible limits.

POLICY & INTERNATIONAL SUPPORT



U.S. MORATORIUM ON DESTRUCTIVE DIRECT-ASCENT ASAT TESTING

Since 2008, the United States has upheld a national moratorium on destructive direct-ascent ASAT tests against satellites.

This policy preserves space safety and sets a responsible example.



BROAD INTERNATIONAL SUPPORT

Many nations support norms and commitments to avoid debris-generating ASAT tests.

Organizations and expert groups continue to advance transparency, confidence-building, and practical steps to reduce space debris.

KEY TAKEAWAYS



DESTRUCTIVE ASAT TESTS
CREATE DEBRIS THAT
OUTLIVES THE ATTACK.



DEBRIS PERSISTS FOR
YEARS OR DECADES AND
ENDANGERS EVERYONE.



ALL MAJOR ASAT TESTS
BY ALL STATES HAVE CREATED
BROADER ENVIRONMENTAL RISK.



RESPONSIBLE BEHAVIOR—including
THE U.S. MORATORIUM—HELPS
PROTECT THE COMMONS OF SPACE.



SAFETY, STABILITY, AND
SUSTAINABLE USE OF SPACE
DEPEND ON OUR CHOICES TODAY.

COUNTERSPACE POLICY, DOCTRINE, AND MILITARY ORGANIZATIONS:

HOW NATIONS PREPARE FOR SPACE CONFLICT



COUNTERSPACE CAPABILITY IS MORE THAN TECHNOLOGY.

Space conflict readiness depends on a whole-of-government and whole-of-force approach that combines policy, doctrine, organizations, training, exercises, and command structures. These elements turn hardware and data into credible, coordinated military capability.



DETER THREATS



DEFEND ASSETS



ASSURE OPERATIONS



SUPPORT ALL MISSIONS

WHAT EACH ELEMENT DOES



POLICY

SETS GOALS AND RULES

- Defines national objectives, interests, and red lines
- Establishes authorities and legal frameworks
- Guides investment priorities and risk management



DOCTRINE

EXPLAINS HOW FORCES OPERATE

- Describes concepts of employment and missions
- Provides principles, tactics, and procedures
- Integrates space with joint and multi-domain operations



ORGANIZATIONS

ASSIGN ROLES AND COMMAND RELATIONSHIPS

- Establishes commands, services, and agencies
- Defines responsibilities and chains of command
- Aligns resources, personnel, and authorities



TRAINING & EDUCATION

DEVELOPS PEOPLE AND TEAMS

- Builds skills in operators, planners, and leaders
- Institutionalizes doctrine and standards
- Strengthens cross-domain understanding



EXERCISES & ALLIANCES

IMPROVE READINESS TOGETHER

- Test plans and procedures
- Validate capabilities and decision-making
- Build interoperability and strengthen deterrence

FROM STRATEGY TO OPERATIONS

1



NATIONAL STRATEGY

Assesses threats and sets objectives for space security and national interests.



2



POLICY & GUIDANCE

Establishes authorities, rules of engagement, funding priorities, and international posture.



3



DOCTRINE & CONCEPTS

Defines how forces operate, integrate, and respond in space and across domains.



4



ORGANIZATIONS & RESOURCES

Build or designate commands and units, staff them, and provide equipment and systems.



5



TRAINING & EXERCISES

Educate, train, and exercise to refine skills, test plans, and build readiness.



6



OPERATIONS & ASSESSMENT

Employ forces to deter, defend, and, if necessary, respond; assess and adapt continuously.

TYPICAL ORGANIZATIONAL FEATURES



NATIONAL SPACE COMMANDS

Plan, command, and control military space operations and integrate space power into national defense.



MILITARY SPACE SERVICES

Manage space forces, support to combatant commands, and service-specific capabilities and missions.



DEFENSE MINISTRIES & AGENCIES

Set policy, oversee budgets, and coordinate national space priorities across government.



JOINT & COMBATANT COMMANDS

Employ space capabilities in support of regional and functional missions.



ALLIED & PARTNER COORDINATION

Share information, align policies, and plan together to enhance collective security.

WHY IT MATTERS



DETER AGGRESSION

Credible posture, clear rules, and resilient capabilities raise costs for adversaries.



PROTECT CRITICAL SERVICES

Safeguards communications, PNT, ISR, and other missions societies rely on.



ENABLE JOINT ALL-DOMAIN OPERATIONS

Space power multiplies force effectiveness across air, land, sea, cyber, and space.



IMPROVE DECISION SPEED AND RESILIENCE

Strong organizations and procedures support rapid, coordinated responses.



BUILD TRUST AND STABILITY

Norms, transparency, and cooperation reduce miscalculation and escalation risks.

KEY TAKEAWAYS



Capability requires more than technology—policy, doctrine, organizations, training, and exercises turn tools into effective military power.



Clear policy sets objectives and rules; doctrine explains how to fight; organizations bring the right people, authorities, and resources together.



Exercises and alliances build readiness, validate plans, and strengthen deterrence with partners.



Effective command structures and coordination across domains and government are essential for success in a conflict.



Investing across all elements creates credible deterrence today and resilience for the future.

DIRECT-ASCENT ASAT WEAPONS:

FROM EARTH-BASED MISSILE TO SATELLITE INTERCEPT



DIRECT-ASCENT ANTI-SATELLITE (ASAT) WEAPONS ARE MISSILES LAUNCHED FROM EARTH WITH THE PURPOSE OF REACHING AND DAMAGING OR DESTROYING A SATELLITE OR OTHER SPACE OBJECT.



TARGET SPACE ASSETS FROM THE GROUND.



CHALLENGE SPACE SYSTEMS AND SERVICES.



CREATE STRATEGIC, OPERATIONAL, AND DEBRIS CONCERNS.

THE DIRECT-ASCENT ASAT PROCESS

1 DETECTION & TRACKING



Sensors detect and track the target to determine its position and track future path.

2 LAUNCH



A ground-based missile is launched toward the target.

3 MIDCOURSE FLIGHT



The missile flies on a ballistic trajectory, guided by onboard systems and/or updates.

4 INTERCEPT



The interceptor reaches the target and uses kinetic impact to damage or destroy it.

5 EFFECTS



The target is disabled or destroyed, potentially creating debris that can threaten other space assets.

COMMON CHARACTERISTICS



VISIBLE LAUNCH

Launch can be detected by other nations' sensors and is often publicly observable.



SHORT ENGAGEMENT WINDOW

Interception opportunities are brief, measured in minutes.



POTENTIALLY DESTRUCTIVE RESULTS

Kinetic impact can disable or destroy high-value space assets.



DEBRIS RISK (KINETIC USE)

Destructive tests and attacks can generate long-lived space debris.

SELECTED HISTORICAL MILESTONES



COLD WAR U.S. WORK

The United States conducted research and development on direct-ascent ASAT concepts and systems during the Cold War.

1985

U.S. ASM-135 TEST

The United States conducted the ASM-135 ASAT test, intercepting a satellite in low Earth orbit.

2007

CHINA DESTRUCTIVE TEST

China conducted a destructive ASAT test against one of its own weather satellites, creating significant space debris.

2019

INDIA MISSION SHAKTI

India successfully conducted Mission Shakti, demonstrating a direct-ascent ASAT capability.



RUSSIA NUDOL PROGRAM

Russia is developing and testing the Nudol direct-ascent ASAT missile as part of its strategic programs.

WHY THEY MATTER



ASAT weapons can be used to deny, degrade, or threaten an adversary's space capabilities.



They can enable broader military operations and coercive strategies.



Their use can escalate conflicts and generate debris that harms all space users.



They drive strategic competition and influence arms control discussions.

ADVANTAGES AND LIMITS



ADVANTAGES

- Relatively simple concept with existing missile technologies.
- Can target a wide range of orbits from the ground.
- Provides a strategic counterspace option.



LIMITS

- Launch is detectable and can be countered.
- Very short time window to execute successfully.
- High risk of space debris if used destructively.
- Political, legal, and strategic consequences are severe.

KEY TAKEAWAYS



DIRECT-ASCENT ASAT WEAPONS ARE MISSILES LAUNCHED FROM EARTH TO DAMAGE OR DESTROY SPACE OBJECTS.



THEY INVOLVE A RAPID, HIGH-STAKES PROCESS FROM DETECTION TO POTENTIAL INTERCEPT.



KINETIC USE CAN CREATE DEBRIS THAT RISKS OTHER SATELLITES AND SPACE OPERATIONS.



THEY POSE STRATEGIC, OPERATIONAL, AND NORMATIVE CHALLENGES FOR THE GLOBAL COMMUNITY.



RESPONSIBLE BEHAVIOR AND TRANSPARENCY ARE ESSENTIAL TO A STABLE AND SUSTAINABLE SPACE ENVIRONMENT.

CO-ORBITAL ASAT SYSTEMS: WHEN THE THREAT IS ALREADY IN SPACE

SATELLITES THAT CAN APPROACH, INSPECT, SHADOW, INTERFERE WITH, MANIPULATE, OR ATTACK OTHER SPACECRAFT



CO-ORBITAL COUNTERSPACE SYSTEMS ARE SPACECRAFT ALREADY IN ORBIT THAT CAN GET CLOSE TO ANOTHER SPACECRAFT AND TAKE ACTION AGAINST IT.



CAN APPROACH AND OBSERVE

Collect intelligence or assess capabilities.



CAN INSPECT OR SHADOW

Fly close to monitor, photograph, or track.



CAN INTERFERE

Use jamming, signals, or other means to disrupt operations.



CAN MANIPULATE

Use robotic tools to contact, disable, or damage components.



CAN ATTACK

Use directed energy, kinetic impact, or other methods to destroy or degrade.

RENDEZVOUS AND PROXIMITY OPERATIONS (RPO)



RPO IS THE ABILITY OF A SPACECRAFT TO NAVIGATE CLOSE TO ANOTHER SPACE OBJECT IN SPACE.

- Essential for docking, servicing, debris removal, assembly, and inspection.
- Dual-use by nature: the same capabilities that enable cooperation can be used to threaten or attack.

INTENT IS HARD TO PROVE. CAPABILITY IS EASY TO BUILD.

HOW CO-ORBITAL SYSTEMS WORK (AT A HIGH LEVEL)

- LAUNCH & DEPLOY**
A spacecraft is placed into orbit with maneuver capability.
- NAVIGATE & RENDEZVOUS**
It maneuvers to reduce distance to the target.
- CLOSE OPERATIONS**
It operates nearby—ranging from hundreds of kilometers to just meters.
- ACTION OPTIONS**
Observe, interfere, manipulate, or attack.
- DISENGAGE OR ESCALATE**
It can depart quietly or remain to sustain effects.

WHY THEY ARE AMBIGUOUS



A CLOSE APPROACH CAN LOOK LIKE INSPECTION OR PREPARATION FOR AN ATTACK.



OBSERVER CANNOT EASILY DETERMINE PAYLOAD FUNCTION OR TRUE INTENT.



ACTIONS ARE OFTEN REVERSIBLE AND MAY ESCALATE SLOWLY.



RELY ON PRECISION TRACKING—MEASUREMENT ERRORS CAN CREATE MISINTERPRETATION.

PEACEFUL VS HOSTILE INTERPRETATIONS



PEACEFUL / LEGITIMATE USES

- On-orbit inspection and verification
- Satellite servicing and refueling
- Component repair or replacement
- Debris removal and graveyarding
- Technology demonstration
- Space situational awareness



HOSTILE / MALICIOUS USES

- Intelligence collection on capabilities
- Stalking, shadowing, or intimidation
- Jamming or communications disruption
- Robotic manipulation or disabling
- Directed energy or other attacks
- Kinetic destruction

KEY COUNTRY EXAMPLES



SOVIET UNION (COLD WAR)

- Deployed co-orbital ASAT systems such as *Is Pilyus* in the 1960s–80s.
- Carried weapons including co-orbital interceptors and nuclear devices.
- Program ended with the collapse of the USSR.



UNITED STATES

- Operates maneuverable satellites for inspection, servicing, and resilience.
- Invests in robotic tools, proximity operations, and responsive space capabilities.
- Maintains these as defensive and for mission assurance.



RUSSIA

- Fielded inspector satellites (e.g., *Kosmos* series) with close-approach capabilities.
- Demonstrated co-orbital behavior raising concern among allies.
- Developing advanced RPO and counterspace tools.



CHINA

- Conducted numerous close approaches and rendezvous operations.
- Shijian series demonstrates robotic arm and inspection capabilities.
- Investing heavily in dual-use and counterspace systems.

MODERN CONCERNS



MANEUVERABLE SATELLITES WITH RPO CAPABILITY ARE MORE COMMON.



ROBOTIC TOOLS ENABLE MANIPULATION WITHOUT DIRECT CONTACT.



INSPECTION MISSIONS CAN COLLECT SENSITIVE TECHNICAL DATA.



CLOSE-APPROACH BEHAVIOR BY MAJOR POWERS DRIVES RISK AND UNCERTAINTY.

ADVANTAGES OF CO-ORBITAL SYSTEMS



STEALTHY & HARD TO ATTRIBUTE

Looks similar to legitimate activity.



PERSISTENT PRESENCE

Can remain in vicinity and act at the time of choice.



MULTIPLE EFFECTS

One system can observe, interfere, manipulate, or attack.



LOW BARRIER TO ESCALATE

Small actions can lead to larger consequences.

DRAWBACKS AND LIMITATIONS



DEPENDENT ON TRACKING

Requires accurate navigation and target data.



VULNERABLE IF DETECTED

May be monitored, countered, or engaged.



LEGAL & POLITICAL RISKS

Violates norms or treaties; leads to diplomatic fallout.



COMPLEX & COSTLY

High development and operational costs.

KEY TAKEAWAYS

- ✓ CO-ORBITAL SYSTEMS BLUR THE LINE BETWEEN PEACEFUL USE AND ATTACK.
- ✓ RENDEZVOUS AND PROXIMITY OPERATIONS ARE DUAL-USE BY DESIGN.
- ✓ AMBIGUOUS ACTIONS CREATE UNCERTAINTY AND ESCALATION RISK.
- ✓ EARLY DETECTION, TRANSPARENCY, AND NORMS ARE CRITICAL.
- ✓ RESILIENCE, REDUNDANCY, AND SPACE DOMAIN AWARENESS ARE ESSENTIAL.

DIRECTED-ENERGY COUNTERSPACE WEAPONS: LASERS, DAZZLERS, AND HIGH-POWER MICROWAVES



DIRECTED-ENERGY COUNTERSPACE TOOLS ARE NON-KINETIC SYSTEMS THAT USE CONCENTRATED ENERGY TO INTERFERE WITH OR DAMAGE PARTS OF SPACE SYSTEMS.

They can degrade, disrupt, or deny the use of satellites and ground infrastructure without the need for physical contact. Effects may be temporary or reversible, or potentially damaging, depending on power, target, exposure time, and conditions.



LASERS

- Use focused light to heat, damage, or disable optical components such as sensors, cameras, and solar cells.
- Effects range from temporary performance degradation to permanent damage based on power and exposure.



SENSOR DAZZLING

- Use lower-power light to overwhelm or blind sensors without causing lasting physical damage.
- Can disrupt imaging, tracking, and communications by reducing sensor effectiveness.



HIGH-POWER MICROWAVES (HPM)

- Use microwave energy to induce currents or voltage spikes in electronics and wiring.
- Can cause temporary disruptions or permanent damage to components and subsystems.

CATEGORY	EFFECTS	DELIVERY OPTIONS	ADVANTAGES	LIMITATIONS
 LASERS	Heat, degrade, or destroy optical sensors, detectors, and solar cells. May cause tracking loss, image artifacts, or permanent damage.	• Ground-based systems • Airborne platforms • Maritime platforms • Space-based systems	• High precision • Scalable effects with power and dwell time • Speed-of-light engagement • Can be difficult to attribute	• Affected by weather, clouds, smoke, and haze • Requires precise targeting and tracking • Line-of-sight only • Power and thermal management needs
 SENSOR DAZZLING	Overwhelms or blinds sensors. Causes temporary loss of tracking, imaging, or communications. Typically non-destructive.	• Ground-based systems • Airborne platforms • Maritime platforms • Space-based systems	• Lower power than damaging lasers • Reversible and adjustable effects • Can create ambiguity and delay • Lower risk of escalation	• May be less effective with hardened sensors • Effect often temporary • Atmospheric conditions reduce performance • May require continuous illumination
 HIGH-POWER MICROWAVES	Induces currents or voltage spikes that disrupt or damage electronics. Can cause temporary outages or permanent failures.	• Ground-based systems • Airborne platforms • Maritime platforms • Space-based systems	• Can affect unshielded or vulnerable electronics • Potential for area or broad effects • Minimal collateral physical damage • Effective against a range of systems	• Requires high power and large antennas • Less precise targeting • Limited by propagation and plasma effects • Attribution can be difficult



WHY THIS MATTERS



Provides a way to impose costs or deny capabilities without physical collision or debris.



Can support deterrence by creating uncertainty about when and how systems may be used.



Can support sensing, communications, and navigation that modern operations depend on.



Attractive to state and non-state actors due to flexibility and scalability across domains.



KEY TAKEAWAYS



Directed-energy tools offer non-kinetic options that can create effects without physical contact.



Targeting is difficult. Atmospheric conditions can degrade performance and limit effectiveness.



Power generation, thermal management, and logistics are major enablers and constraints.



Attribution remains challenging, complicating escalation management and response.

COMMERCIAL SPACE IN THE CROSSHAIRS: WHEN CIVILIAN SATELLITES SUPPORT MILITARY OPERATIONS



COMMERCIAL SPACE POWERS MODERN LIFE

Private companies operate satellites and provide services that underpin communications, navigation, timing, Earth observation, data, and cloud connectivity.



DUAL-USE BY DESIGN

These services support national security missions as well as the global economy and everyday life.



STRATEGIC AMBIGUITY

Systems may be privately owned and commercially operated, yet their loss, disruption, or denial can affect military operations and civilian life alike.

WHY COMMERCIAL SPACE MATTERS



Scales capability rapidly and cost-effectively.



Provides global coverage and persistent access.



Delivers innovation and continuous improvement.



Extends government reach through partnerships.



Supports economic growth and quality of life.

COMMON SERVICES



COMMUNICATIONS

Voice, data, broadband and tactical links



EARTH OBSERVATION

Imagery, mapping, monitoring and change detection



TIMING & SYNCHRONIZATION

Precise time for networks, finance, power and military systems



NAVIGATION SUPPORT

PNT augmentation and resiliency for critical applications



CLOUD & DATA SERVICES

Storage, processing, analytics and AI at scale



OTHER FUNCTIONS

Space domain awareness, relay, weather and more

WHY COMMERCIAL SYSTEMS CAN BECOME TARGETS



They are critical enablers of military operations and decision-making.



They are exposed across large geographic areas and users.



They represent valuable infrastructure and intellectual property.



They may be visible, predictable, or have limited defensive measures.



They rely on complex supply chains and third-party providers.

TYPES OF RISKS



JAMMING

Deliberate signals disrupt or deny legitimate communications and services.



CYBERATTACK

Intrusions, malware or data theft can compromise systems and services.



INTERFERENCE

Unintentional or malicious interference degrades or blocks performance.



PHYSICAL ATTACK

Kinetic or directed-energy attacks can damage or destroy space or ground assets.



SUPPLY-CHAIN VULNERABILITY

Weaknesses in parts, software, logistics or providers can be exploited.

IMPACTS OF AN ATTACK ON COMMERCIAL SYSTEMS



EFFECTS ON MILITARY OPERATIONS

- Loss of communications and data links
- Reduced situational awareness
- Degraded precision and timing
- Slower command and decision cycles
- Mission delays or failure



EFFECTS ON CIVILIANS

- Disrupted internet and mobile services
- Impaired navigation and transportation
- Delays in emergency response
- Financial and economic disruption
- Reduced access to critical services



AN ATTACK ON COMMERCIAL SPACE IS AN ATTACK ON BOTH NATIONAL SECURITY AND THE PEOPLE WHO RELY ON IT.

WHY RESILIENCE IS IMPORTANT



Maintains mission assurance and continuity of operations.



Builds layered, redundant and diverse architectures.



Strengthens cyber and supply-chain security.



Enables public-private coordination and information sharing.



Protects the economy, society and national security.



KEY TAKEAWAYS



COMMERCIAL SPACE IS ESSENTIAL TO MILITARY AND CIVILIAN LIFE.



DUAL-USE SERVICES CREATE STRATEGIC AMBIGUITY AND POTENTIAL VULNERABILITIES.



ADVERSARIES CAN EXPLOIT MULTIPLE AVENUES TO DENY, DISRUPT OR DEGRADE SERVICES.



IMPACTS CAN SPAN FROM THE BATTLEFIELD TO EVERYDAY CIVILIAN ACTIVITIES.



RESILIENCE, PARTNERSHIPS AND INNOVATION ARE KEY TO DETER AND RECOVER.

PROLIFERATED LEO CONSTELLATIONS:

RESILIENCE VERSUS THE NEXT GENERATION OF COUNTERSPACE WEAPONS

WHAT ARE PROLIFERATED LEO CONSTELLATIONS?



Proliferated constellations use hundreds to thousands of small, lower-cost satellites in low Earth orbit (LEO) working together as an integrated system. Instead of a few large, exquisite spacecraft, many smaller satellites share the mission—spreading risk and providing global, persistent service.

WHY GOVERNMENTS AND COMMERCIAL OPERATORS VALUE THEM



PERSISTENCE

Service continues when individual satellites are lost.



REDUNDANCY

Multiple paths and assets reduce single points of failure.



RESILIENCE

Harder to disrupt or defeat the entire system.



FASTER REPLACEMENT

Smaller satellites can be built, launched, and replenished faster.



LOWER UNIT COST

Economies of scale reduce cost per capability.



THE CHALLENGE: ADVERSARIES MAY SEEK TO DISRUPT MANY SATELLITES OR THEIR SUPPORTING NETWORKS AT ONCE

As constellations grow in size and importance, so does the incentive to interfere with them. Adversaries are investing in capabilities that can target new ways—ranging from reversible disruption to potentially destructive attacks.



ELECTRONIC WARFARE

Jamming, spoofing, and deception can deny or degrade communications and navigation.



CYBER OPERATIONS

Intrusions against ground infrastructure, networks, supply chains, and software can disrupt services at scale.



POTENTIALLY DISRUPTIVE STRATEGIES

Directed energy, co-orbital systems, and kinetic attacks could degrade or destroy multiple satellites.

BENEFITS OF PROLIFERATION



DISTRIBUTED SURVIVABILITY: No single satellite is critical; loss of some does not end the mission.



GLOBAL COVERAGE: Large constellations deliver continuous service across wide areas and to many users.



SCALABLE CAPACITY: More satellites add capacity and performance over time.



COST EFFICIENCY: Lower-cost satellites and rideshare launches reduce the cost to field and refresh the system.



RAPID INNOVATION: Modular designs and shorter development cycles enable faster iteration and technology insertion.

VULNERABILITIES TO EXPLOIT



SIGNAL DEPENDENCE: Reliance on radio links that can be jammed, spoofed, or intercepted.



GROUND SEGMENT EXPOSURE: Ground stations, gateways, and data centers are attractive targets.



SOFTWARE AND SUPPLY CHAIN RISK: Bugs, backdoors, and compromised updates can cascade across large fleets.



CONSTELLATION-SCALE ATTACKS: Effects that are modest against one satellite can become mission-impacting when applied across many.



LAUNCH AND REPLENISHMENT WINDOWS: Launch cadence and on-orbit reconstitution create time-sensitive vulnerabilities.

WHAT COUNTERSPACE ADAPTATION MAY LOOK LIKE



SPECTRUM COMPETITION: Persistent EW to deny, degrade, or deceive communications and navigation.



CO-ORBITAL AND KINETIC CAPABILITIES: Systems designed to approach, damage, or destroy multiple satellites or key nodes.



DIRECTED ENERGY: High-power systems to dazzle, degrade, or damage sensors and electronics.



CYBER AND SUPPLY CHAIN OPERATIONS: Penetrate networks, exploit trusted software, or manipulate data and commands.



MULTI-DOMAIN, MULTI-VECTOR CAMPAIGNS: Combining EW, cyber, and kinetic effects to overwhelm defenses and decision cycles.

CONCERN IS GROWING



Policymakers and operators increasingly recognize that defeating or degrading proliferated constellations is a distinct military objective. The scale, connectivity, and commercial relevance of these systems mean their disruption could yield strategic, economic, and information advantages in a crisis or conflict.

KEY TAKEAWAYS



PROLIFERATION DRIVES RESILIENCE, BUT NOT IMMUNITY.

Large numbers reduce risk but create new attack surfaces.



RESILIENCE REQUIRES MORE THAN NUMBERS.

It depends on secure links, hardened networks, and trusted supply chains.



COUNTERSPACE IS EVOLVING.

Adversaries are investing in capabilities to target many nodes at once.



ADAPTATION IS ESSENTIAL.

Design for contest, assume disruption, and plan for rapid reconstitution.



PARTNERSHIPS MATTER.

Information sharing, standards, and industry-government collaboration strengthen deterrence and resilience.

PEACETIME NORMS VS. WARTIME SPACE OPERATIONS: PREVENTING MISCALCULATION AND ESCALATION



RESPONSIBLE STATE BEHAVIOR IN SPACE IS CRITICAL AT ALL TIMES. MANY NORMS AND PROPOSALS GUIDE PEACETIME ACTIVITIES. DURING CONFLICT, STATES MAY STILL SEEK TO DISRUPT OR DEGRADE ADVERSARY SPACE CAPABILITIES.



CLEAR NORMS AND COMMUNICATION
REDUCE MISCALCULATION AND HELP KEEP
ROUTINE INCIDENTS FROM BECOMING CRISES.

RESPONSIBLE SPACE CONDUCT IN PEACETIME



SAFE SEPARATION

Operate to avoid collisions and keep appropriate distance between objects.



ADVANCE NOTIFICATIONS

Share timely information about launches, maneuvers, and other significant events.



AVOID HARMFUL INTERFERENCE

Refrain from actions that disrupt or degrade others' space systems or services.



LIMIT LONG-LIVED DEBRIS

Design, operate, and dispose to minimize space debris and associated risks.



CLEAR COMMUNICATION

Use transparent, professional channels to share information and resolve concerns.

WHY NORMS MATTER



REDUCE MISUNDERSTANDING

Shared expectations and predictable behavior lower the chance of mistaken intent and false alarms.



BUILD TRANSPARENCY

Information sharing and communication create visibility into activities and intentions.



LOWER ESCALATION RISK

Clear boundaries and professional conduct limit incentives for retaliation and help keep crises local.

FOUNDATIONAL INITIATIVES SUPPORTING RESPONSIBLE BEHAVIOR



U.S. RESPONSIBLE-BEHAVIOR TENETS

The United States advances voluntary tenets for responsible military behavior in space to promote safety, stability, and the long-term sustainability of the space environment.



USSPACECOM PROPOSED BEHAVIORS

USSPACECOM has proposed voluntary behaviors for space operations to reduce risk, improve accountability, and strengthen strategic stability.



MORATORIUM MOVEMENT

Many states support a moratorium on destructive, direct-ascent ASAT testing that creates long-lived debris, which poses risks to all space users.

PEACETIME VS. WARTIME: DIFFERENT CONTEXT, DIFFERENT DYNAMICS

DIMENSION	PEACETIME	WARTIME
 OBJECTIVES	Sustain services, safety, and stability.	Gain advantage; deny, disrupt, or degrade adversary capabilities.
 INTENT SIGNALS	Transparency, notifications, and consultations.	Deception, ambiguity, and limited or no notifications.
 TOLERANCE FOR RISK	Low tolerance for actions that create danger or destabilize.	Higher willingness to accept risk, collateral effects, and escalation.
 BEHAVIOR	Cooperative norms guide planning and operations.	Competitive and conflicting behaviors may be employed.
 ESCALATION PATHWAYS	Robust norms and communication reduce misunderstanding and escalation.	Stress, speed, and uncertainty increase risk of miscalculation and escalation.

KEY TAKEAWAYS



NORMS ARE NOT A SUBSTITUTE FOR DETERRENCE, ALLIANCES, OR DEFENSE, BUT THEY ARE A CRITICAL LAYER OF RISK REDUCTION.



PEACETIME NORMS SET EXPECTATIONS; WARTIME BEHAVIORS MAY DEVIATE. CLARITY HELPS STATES RESPOND CALMLY.



COMMUNICATION, TRANSPARENCY, AND RESTRAINT REDUCE THE CHANCES THAT ROUTINE INCIDENTS BECOME STRATEGIC CRISES.



INVESTING IN NORMS TODAY STRENGTHENS STABILITY AND KEEPS SPACE ACCESSIBLE, SECURE, AND SUSTAINABLE FOR ALL.

CHINA'S COUNTERSPACE STRATEGY AND SPACE FORCE REORGANIZATION

BUILDING CAPABILITIES, GAINING PROFICIENCY, SHAPING THE FUTURE OF CONFLICT IN SPACE



CHINA HAS PLACED GROWING EMPHASIS ON THE MILITARY USE OF SPACE. IT HAS DEMONSTRATED DUAL-USE, HIGHLY MANEUVERABLE SATELLITES AND INCREASINGLY SOPHISTICATED RENDEZVOUS AND PROXIMITY OPERATIONS. OPERATOR PROFICIENCY, AGGRESSIVE MANEUVERING, AND MATURING SPACE TACTICS ARE MAJOR THEMES.



SPACE FORCE REORGANIZATION

CHINA HAS REORGANIZED ITS ARMED FORCES AND CREATED A FORCE ORIENTED AROUND SPACE OPERATIONS.

- ✓ Centralized leadership and authorities
- ✓ Integrated planning and operations
- ✓ Focus on multi-domain, joint warfighting



CORE THEMES

- Operator proficiency is improving
- Aggressive and purposeful maneuvering
- Maturing tactics and doctrines
- Preparation for contested space operations

CHINA'S COUNTERSPACE CAPABILITY AREAS



MANEUVERABLE SATELLITES AND RPO

- Demonstrated proximity operations in multiple orbits, including GEO.
- Satellites exhibit capabilities for inspection, positioning, and potential interference.
- Repeated missions build experience and confidence.



DIRECT-ASCENT ASAT HISTORY

- Conducted direct-ascent ASAT test against a defunct satellite.
- Demonstrates willingness to use destructive kinetic means.
- Signals a capability to threaten satellites across orbits.



ELECTRONIC WARFARE

- Jamming, spoofing, and deception can degrade, deny, or disrupt space capabilities.
- Supports deny, disrupt, degrade, and disrupt (D4) operations.



CYBER ACTIVITY

- Cyber operations can target satellite systems, ground stations, and networks.
- Potential to steal data, disrupt services, or implant persistent access.



SPACE SITUATIONAL AWARENESS (SSA)

- Extensive sensors, tracking networks, and data fusion enhance awareness.
- SSA underpins targeting, maneuver planning, and mission execution.



BROADER MILITARY-SPACE STRATEGY

- Space integrated into overall military strategy.
- Aim: deny adversary use of space while ensuring freedom of action for China.
- Supports asymmetric advantage in conflict.

WHY DUAL-USE TECHNOLOGIES COMPLICATE INTERPRETATION



Technologies serve commercial, civilian, and military purposes, blurring intent.



Same capabilities can support benign services or counterspace missions.



Ambiguity raises uncertainty and complicates attribution and response.



Norms and verification are limited in space.

KEY MILESTONES



2007 DIRECT-ASCENT ASAT DEMONSTRATION

China conducts a kinetic ASAT test against a defunct satellite.



2010s GROWING RPO AND MANEUVER ACTIVITY

Proximity operations increase across LEO and GEO.



LATE 2010s-EARLY 2020s GEO MANEUVER SOPHISTICATION

More complex maneuvers demonstrate precision, endurance, and control.



2020-PRESENT SPACE FORCE REORGANIZATION

Creation of a dedicated Space Force and centralized authorities.

WHY THIS MATTERS



Undermines deterrence by creating ambiguity about intent and capabilities.



Raises miscalculation risks during crises or conflict.



Challenges U.S. and allied access to critical space services.



Drives need for resilience, domain awareness, partnerships, and clear responses.



KEY TAKEAWAYS



China is investing heavily in counterspace capabilities across multiple domains.



Operator proficiency and sophisticated maneuvers are key accelerants.



Integrated capabilities create layered options to deny, disrupt, or degrade adversary space assets.



Dual-use and ambiguity complicate interpretation and response.



Deterrence, resilience, and allied cooperation are essential to protect space interests.

RUSSIA'S CO-ORBITAL THREAT: INSPECTORS, SHADOWING, AND PROXIMITY OPERATIONS

A LONG HISTORY OF CO-ORBITAL ANTI-SATELLITE CONCEPTS—TODAY'S AMBIGUITY CREATES TOMORROW'S RISK



Russia has decades of experience with co-orbital anti-satellite (ASAT) concepts. Modern activity includes inspector satellites, close approaches, and spacecraft that shadow or maneuver near other satellites.

SOME BEHAVIOR CAN SUPPORT PEACEFUL INSPECTION OR SURVEILLANCE MISSIONS—BUT CAN ALSO SUPPORT COUNTERSPACE OPERATIONS.

MODERN RUSSIAN CO-ORBITAL ACTIVITY: PATTERNS AND EXAMPLES

INSPECTOR SATELLITES



- Dedicated "inspector" satellites designed for proximity operations.
- Repeated launches of inspector-class spacecraft since the 2010s.

CLOSE APPROACHES



- Maneuvering near other satellites in LEO and GEO.
- Includes short-range approaches and orbital plane changes.

SHADOWING & ESCORTING



- Following or loitering near other satellites for extended periods.
- Observed in LEO and GEO, including with foreign military satellites.

SUB-SATELLITE DEPLOYMENT CONCERNS



- Testing of released objects in LEO and GEO raises concerns.
- Could enable sensors, effectors, or other payloads.

DUAL-USE BY DESIGN: AMBIGUITY IS THE ADVANTAGE



PEACEFUL PURPOSES

- On-orbit inspection & verification
- Space situational awareness (SSA)
- Technology demonstration & proximity operations
- Satellite servicing support



POTENTIAL MILITARY USES

- Intelligence, surveillance, & reconnaissance
- Electronic interference & collection
- Disabling or damaging targets
- Positioning for attack or sub-satellite release



THE SAME CAPABILITIES THAT SUPPORT PEACEFUL MISSIONS CAN BE RAPIDLY REPURPOSED FOR COUNTERSPACE OPERATIONS.

FROM SOVIET CO-ORBITAL ASAT HERITAGE TO TODAY'S PROXIMITY OPERATIONS

1960s–1980s

SOVIET ERA



Co-orbital ASAT concepts and studies; early inspection and interceptor ideas.

1990s

POST-SOVIET CONTINUITY



Research continues; heritage knowledge and facilities preserved.

2000s

EARLY PROGRAM DEVELOPMENT



New co-orbital programs emerge; prototype and technology work.

2010s

INSPECTORS & TESTING



Launches of inspector satellites; RPO tests in LEO and GEO; proximity ops observed.

2020s

PERSISTENT PROXIMITY OPS



Ongoing close approaches, shadowing, and RPO missions continue.

★ Open-source reporting highlights RPO testing in both LEO and GEO and behavior linked to programs such as Luch/Olymp in GEO. Intent remains unclear; patterns suggest continued investment and operational refinement.

WHY ATTRIBUTION AND INTENT ARE HARD TO READ



LIMITED TRANSPARENCY

Space is hard to observe. Many behaviors are not visible from the ground.



DUAL-USE CAPABILITIES

Same platforms and maneuvers can serve benign or hostile missions.



PLAUSIBLE DENIABILITY

Close approaches and deployments can be framed as "inspection" or "experimentation."



INDIRECT EVIDENCE

Attribution relies on patterns, history, and inference—not definitive proof.



INTENT CHANGES OVER TIME

A benign mission today could be used for attack tomorrow.

OPERATIONAL RISKS: MORE THAN JUST SATELLITE THREATS



INTIMIDATION AND COERCION

Proximity operations create pressure and signal capability, undermining confidence.



MISCALCULATION AND COLLISION

Close operations increase collision risk and the chance of misreading intent.



INTERFERENCE AND DISRUPTION

Potential for electronic interference, data exfiltration, or disabling actions.



CRISIS ESCALATION

Ambiguous actions can trigger rapid reaction, countermeasures, and escalation spirals.



CO-ORBITAL OPERATIONS LOWER THE THRESHOLD FOR CONFLICT AND COMPLICATE STABILITY IN SPACE.



KEY TAKEAWAYS

1

A LONG HERITAGE

Soviet-era concepts laid the foundation for today's co-orbital capabilities.

2

ACTIVE AND EVOLVING

Russia continues to test, field, and refine inspector, RPO, and shadowing capabilities in LEO and GEO.

3

AMBIGUITY IS STRATEGIC

Dual-use designs make it difficult to determine intent and harder to deter.

4

MONITOR, SHARE, PREPARE

Persistent monitoring, information sharing, and resilient operations reduce surprise and risk.

5

DETER TO PRESERVE STABILITY

Clear signaling of costs, norms of responsible behavior, and credible capabilities are essential to deter aggression in space.



GPS JAMMING AND SPOOFING HOTSPOTS: THE COUNTERSPACE THREAT PEOPLE CAN FEEL ON EARTH

GNSS SIGNALS POWER MODERN LIFE. INTERFERENCE CAN DISRUPT IT IN AN INSTANT.

JAMMING vs SPOOFING: KNOW THE DIFFERENCE



JAMMING

BLOCKS OR OVERWHELMS RECEPTION OF GNSS SIGNALS.

- DROWNS OUT LEGITIMATE SIGNALS
- RECEIVER LOSES POSITION, SPEED, AND TIME
- EFFECT IS IMMEDIATE AND OFTEN OBVIOUS



SPOOFING

CAUSES RECEIVERS TO ACCEPT FALSE LOCATION OR TIMING INFORMATION.

- IMITATES REAL GNSS SIGNALS
- RECEIVER SHOWS WRONG BUT PLAUSIBLE DATA
- HARDER TO DETECT AND POTENTIALLY DANGEROUS

WHY GNSS SERVICES MATTER EVERYWHERE



AVIATION

Safe navigation, precise approaches, and timing



SHIPPING

Route guidance, port operations, and timing



EMERGENCY SERVICES

Dispatch, response coordination, and situational awareness



TELECOM NETWORKS

Network synchronization, cell timing, and location services



AGRICULTURE

Precision farming, autosteer, and yields



POWER SYSTEMS

Grid synchronization, phasor measurement, and protection



EVERYDAY NAVIGATION

Maps, rideshare, logistics, fitness, and personal safety apps



FINANCIAL SERVICES

High-frequency trading, timestamping, and audit trails

WHERE INTERFERENCE HAS BEEN PROMINENT (RECENT YEARS)



NORDIC AND BALTIC REGION

Frequent jamming impacting aviation, maritime, and ground users across the Baltic Sea and beyond.



UKRAINE AND RUSSIA

Extensive jamming and spoofing affecting military and civilian users throughout the conflict area.



THE MIDDLE EAST

Widespread jamming and spoofing affecting aircraft and maritime navigation, especially near conflict zones.



KOREAN PENINSULA

Interference incidents impacting military activities and civilian navigation in the region.



SOUTH ASIA

Increasing reports of jamming and spoofing affecting aviation, maritime, and land operations.



INTERFERENCE HAS AFFECTED AIRCRAFT AND MARITIME NAVIGATION AND HAS BECOME MORE WIDESPREAD AROUND CONFLICT ZONES.

THE GROWING TREND



SIGNIFICANT INCREASE

IN REPORTED GNSS INTERFERENCE EVENTS IN THE LAST 5 YEARS.



HOW INTERFERENCE HAPPENS

1

INTENT

An actor decides to disrupt or deceive GNSS users.

2

EQUIPMENT

Portable or fixed devices generate jamming noise or spoofing signals.

3

TRANSMISSION

Signals are sent toward the target area, overpowering or imitating satellites.

4

RECEIVER IMPACT

Receivers lose signal (jamming) or accept false data (spoofing).

5

REAL-WORLD EFFECTS

Navigation errors, delays, incidents, economic loss, and safety risks.

WHY IT IS HARD TO STOP



LOW COST, EASY TO USE

Commercial-off-the-shelf devices are affordable and widely available.



MOBILE AND HARD TO FIND

Devices can be small, moved frequently, and operated briefly.



HARD TO ATTRIBUTE

Signals can look similar to natural noise and are hard to trace.



LEGAL AND POLICY CHALLENGES

Spectrum laws, jurisdiction issues, and international coordination limits.



DETECTING SPOOFING IS HARD

Spoofed signals can appear valid to standard receivers.

KEY TAKEAWAYS: BUILD RESILIENCE, STAY ALERT, REPORT



BUILD RESILIENCE

Use multi-constellation (GPS, Galileo, GLONASS, BeiDou, and others) and modernized receivers.



USE BACKUPS

Combine GNSS with alternative PNT sources: inertial systems, terrain, visual, and radio aids.



MONITOR AND DETECT

Deploy monitoring tools, train personnel, and act on anomaly alerts.



PLAN AND TRAIN

Include GNSS denial scenarios in plans, exercises, and drills.



REPORT INCIDENTS

Report interference to authorities and trusted networks. Your report helps others.



COLLABORATE

Share data, coordinate responses, and support strong policies to protect the PNT ecosystem.



GNSS INTERFERENCE IS A REAL AND GROWING THREAT. AWARENESS, PREPAREDNESS, AND COOPERATION ARE OUR BEST DEFENSE.

CYBER WARFARE AGAINST SPACE SYSTEMS: THE DRIP-DRIP OF ATTACKS

PERSISTENT. CUMULATIVE. DISRUPTIVE. SILENT TODAY, STRATEGIC TOMORROW.

WHAT CAN BE TARGETED



SPACECRAFT

Onboard computers, sensors, actuators and payloads



GROUND STATIONS

Telemetry, tracking, telecommand and uplinks



MISSION-CONTROL NETWORKS

Operations centers, networks and engineering systems



USER TERMINALS

End-user devices and access applications



SOFTWARE

Flight software, applications, firmware



SUPPLY CHAINS

Hardware, software, vendors and third-party services



DATA LINKS

Uplinks, downlinks and crosslinks (when used)



CLOUD & ENTERPRISE SYSTEMS

Data storage, analytics, IT services and business systems

END-TO-END SPACE SYSTEM ARCHITECTURE (ATTACK SURFACE CHAIN)



SPACECRAFT

Collects data and executes missions



GROUND STATIONS

Receives data, sends commands



MISSION-CONTROL NETWORKS

Plans, monitors and manages operations



USER TERMINALS

Access services and data



CLOUD & ENTERPRISE SYSTEMS

Store, process and distribute data

SUPPORTING FOUNDATIONS ACROSS ALL NODES



SOFTWARE



SUPPLY CHAINS



DATA LINKS



IDENTITIES



THIRD PARTIES

MAJOR CYBER ATTACK TYPES



ESPIONAGE

Steal sensitive data, intellectual property or mission details for strategic advantage.



DISRUPTION

Interfere with services or operations without permanently destroying systems.



RANSOMWARE

Encrypt systems or data to extort payment or concessions.



DENIAL OF SERVICE

Overwhelm or exhaust systems or networks to make services unavailable.



COMMAND INTERFERENCE

Alter, delay or spoof commands to change system behavior.



DATA CORRUPTION

Modify, delete or manipulate data to degrade trust and decision-making.



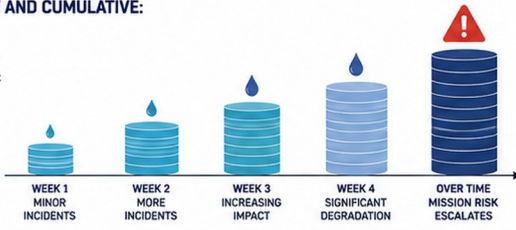
SUPPLY-CHAIN COMPROMISE

Insert malicious code or hardware through vendors or updates.

WHY THE THREAT IS PERSISTENT AND CUMULATIVE: THE DRIP-DRIP OF INCIDENTS



- Small incidents occur regularly.
- Each may cause limited impact on its own.
- Over time they degrade availability, accuracy, integrity and trust.
- Adversaries learn, persist and expand access.
- The cumulative effect can cripple missions and deter decision-makers.



NO SINGLE ATTACK MAY BE CATASTROPHIC—BUT THE AGGREGATE EFFECT CAN BE.

WHY ATTRIBUTION IS DIFFICULT



- Attackers hide behind proxies, stolen identities and compromised infrastructure.
- Use of living-off-the-land tools leaves minimal traces.
- Overlapping tactics and global Internet make source unclear.
- Political risk and limited evidence hinder public attribution.

WHY NON-DESTRUCTIVE INCIDENTS ARE STRATEGICALLY IMPORTANT



- Enable intelligence collection and capability development.
- Pre-position access for future, larger operations.
- Test defenses and map response times.
- Erode confidence in services and decision-making.
- Create uncertainty and impose economic and insurance costs.

DEFENSES: BUILDING RESILIENCE EVERY DAY



SEGMENTATION
Limit lateral movement.



ENCRYPTION
Protect data in transit and at rest.



ZERO TRUST
Verify explicitly, least privilege access.



PATCHING
Keep systems and software up to date.



SUPPLY-CHAIN VETTING
Know your vendors and verify integrity.



CYBER HYGIENE
Strong access controls and user awareness.



ANOMALY DETECTION
Monitor, detect and alert early.



INCIDENT RESPONSE
Prepare, contain, recover and improve.



KEY TAKEAWAYS

- SPACE SYSTEMS ARE HIGH-VALUE, NETWORKED AND DEPENDENT ON COMPLEX DIGITAL ECOSYSTEMS—ATTRACTIVE TARGETS.
- ADVERSARIES USE A BROAD RANGE OF CYBER ATTACKS THAT CAN STEAL, DISRUPT, DEGRADE OR MANIPULATE SYSTEMS.
- THREATS PERSIST AS A DRIP-DRIP OF INCIDENTS THAT ACCUMULATE OVER TIME, NOT AS A SINGLE DRAMATIC STRIKE.
- ATTRIBUTION IS HARD, BUT EVEN NON-DESTRUCTIVE INCIDENTS CARRY MAJOR STRATEGIC CONSEQUENCES.
- RESILIENCE COMES FROM DEFENSE-IN-DEPTH, CONTINUOUS MONITORING AND RAPID RESPONSE.
- CYBER ATTACKS OFTEN OFFER ADVERSARIES A LOWER-BARRIER, LOWER-RISK COUNTERSPACE OPTION THAN KINETIC ATTACK.

IRAN'S GROWING SPACE AND COUNTERSPACE TOOLKIT

BUILDING CAPABILITIES THAT CAN DISRUPT, DENY, AND CREATE RISK IN SPACE AND BEYOND



IRAN IS NOT USUALLY TREATED AS A TOP-TIER SPACE POWER. HOWEVER, ITS PROGRESS IN SPACE LAUNCH AND MISSILE TECHNOLOGY, ELECTRONIC WARFARE CAPABILITIES, AND GROWING INTEREST IN MILITARY SPACE SUPPORT RAISE COUNTERSPACE CONCERNS.



MANY CAPABILITIES ARE LIMITED OR INDIRECT COMPARED TO THE UNITED STATES, RUSSIA, OR CHINA, BUT CAN STILL CREATE OPERATIONAL DISRUPTION OR REGIONAL RISK.

KEY ELEMENTS OF IRAN'S SPACE AND COUNTERSPACE TOOLKIT



LAUNCH VEHICLES & MISSILE OVERLAP

- Space launch vehicles share technology with ballistic missiles.
- Iran's launcher progress advances range, payload, and solid-fuel capabilities.
- Dual-use expertise shortens paths to more capable missile systems.



ELECTRONIC WARFARE & JAMMING POTENTIAL

- Strong domestic EW industry with experience in jamming communications and GNSS.
- Can degrade satellite links, navigation, and ISR support in a region.
- Mobile and adaptable systems complicate detection and attribution.



SPACE SITUATIONAL AWARENESS LIMITATIONS

- Developing sensors and radar with limited reach and precision.
- Incomplete tracking of objects in orbit.
- SSA gaps limit ability to target, warn, or protect in contested space.



CYBER RISK TO SPACE SYSTEMS

- Growing cyber capabilities and proven activity against networks.
- Potential to target satellite operators, ground stations, and supply chains.
- Cyber tools offer low-cost options for disruption below the threshold.



REGIONAL STRATEGIC CONTEXT

- Iran leverages proxies and partners to extend reach and create ambiguity.
- Counters U.S. and allied presence and freedom of action.
- Seeks deterrence and bargaining power through space-related risks.

MILESTONES IN IRAN'S SPACE AND COUNTERSPACE TRAJECTORY



2009

FIRST SATELLITE LAUNCH

Omid satellite launched on the Safir launcher. Symbolic start of Iran's space program.



2011-2013

EARLY FOLLOW-ON LAUNCHES

Additional satellite launch attempts and incremental improvements in launch capability.



2015

NUCLEAR AGREEMENT (JCPOA)

Space and missile programs continue separately from nuclear negotiations; concerns persist.



2019

MILITARY SPACE RHETORIC RISES

Iranian officials call for greater use of space for defense and strategic applications.



2020-2022

NEW LAUNCH VEHICLES & ADVANCEMENTS

Introduction of more capable launchers (e.g., Simorgh, Qaem) and improved solid-fuel motors.



2023-PRESENT

GROWING CONCERNS ABOUT INTERFERENCE

Increased reporting on jamming activity, cyber threats, and interest in counterspace capabilities by Iran.

WHAT IRAN CAN DO

VS.

WHAT IRAN STILL LACKS

- ✓ Launch small satellites into low Earth orbit.
- ✓ Develop and test dual-use technologies that improve missile systems.
- ✓ Conduct electronic warfare and jamming against communications, GNSS, and commercial links.
- ✓ Use cyber tools to target space-related networks and infrastructure.
- ✓ Create uncertainty and impose costs on adversary operations in the region.

- ✗ Reliable, high-capacity launch to higher orbits.
- ✗ Advanced ISR satellites or a resilient satellite constellation.
- ✗ Long-range, precise counterspace weapons (kinetic or directed energy).
- ✗ Comprehensive space situational awareness and tracking.
- ✗ Industrial scale, sustained investment, and global partnerships.

KEY TAKEAWAYS



ASYMMETRY, NOT PARITY

Iran does not match the space power of the U.S., Russia, or China, but pursues asymmetric tools that can still impose meaningful disruption.



REGIONAL LEVERAGE

Targeted jamming, cyber operations, and missile capabilities can degrade adversary advantages and strengthen Iran's deterrence and bargaining power.



OPERATIONAL DISRUPTION

Even temporary interference with communications, navigation, or ISR can disrupt military and civil operations in a crisis.



MONITOR EMERGING CAPABILITIES

Rapid improvements in launch, EW, and cyber tools warrant sustained intelligence, tracking, and analysis.



PREPARE AND RESILIENT

Strengthen space system resilience, redundancy, and defensive options to deter, deny, and mitigate counterspace risks.

NORTH KOREA'S SPACE AMBITIONS AND INTERFERENCE RISKS

SPACE AND MISSILE ACTIVITIES WITH DIRECT SECURITY RELEVANCE TO THE REGION

1. LAUNCH INFRASTRUCTURE & SATELLITE AMBITIONS



Launch sites and test facilities support periodic long-range rocket launches.



North Korea seeks capabilities for reconnaissance, communications, and technological status.



Incremental progress with satellite components, payloads, and launch experience.



Objective: greater autonomy in space-based military and intelligence applications.

SPACE AMBITIONS AT A GLANCE



Reliable access to space via long-range launches



Deploy satellites for observation and communications



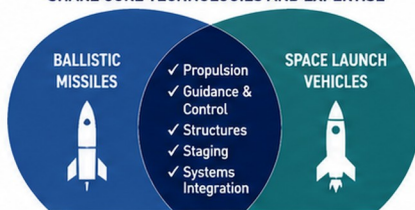
Advance space technology and domestic industrial base



Enhance strategic leverage and regime security

2. OVERLAP: MISSILE TECHNOLOGY = LAUNCH TECHNOLOGY

BALLISTIC MISSILES AND SPACE LAUNCH VEHICLES SHARE CORE TECHNOLOGIES AND EXPERTISE



PROGRESS IN ONE DOMAIN ACCELERATES PROGRESS IN THE OTHER, ENHANCING RANGE, PAYLOAD, AND RELIABILITY OVER TIME.

3. REGIONAL GPS INTERFERENCE CONCERNS



Reports of GPS jamming and spoofing affecting civil and military users in the region.



Impacts navigation, aviation, maritime operations, and critical infrastructure.



Interference escalates in crises and complicates response and attribution.

EFFECTS OF INTERFERENCE



DISRUPTED NAVIGATION



MARITIME RISK



COMMUNICATIONS DEGRADATION



ECONOMIC & SAFETY IMPACTS

LOW COST, HIGH IMPACT, HARD TO ATTRIBUTE

4. MILITARY & INTELLIGENCE IMPLICATIONS



ENHANCED AWARENESS

Satellites can improve surveillance of military activities and targets.



TARGETING SUPPORT

Better data enables more precise planning and strike coordination.



COMMAND & CONTROL

Space assets can strengthen communications resilience.



DETERRENCE & COERCION

Ambiguity and reach complicate defense planning and escalation control.

INTELLIGENCE VALUE



EO/IR imaging for troop movements and facilities



SIGINT payloads for communications collection



Data relay to support real-time operations



EVEN LIMITED CAPABILITIES CAN YIELD HIGH-VALUE INTELLIGENCE PAYOFFS.

5. WHY LIMITED SPACE CAPABILITIES CAN HAVE OUTSIZED STRATEGIC VALUE



STRATEGIC SIGNALLING

Demonstrates capability, intent, and technological momentum.



DIPLOMATIC LEVERAGE

Creates bargaining chips in negotiations and crises.



ASYMMETRIC ADVANTAGE

Exploits vulnerabilities at lower cost than adversaries.



OPTION VALUE

Keeps future military and civil applications on the table.



PERCEPTION CAN BE AS POWERFUL AS POSSESSION.

Ambiguity about true capabilities complicates deterrence and defense planning.

6. WHY OBSERVERS WATCH BOTH ORBITAL & TERRESTRIAL ACTIVITY



SPACE LAUNCHES



TECHNOLOGY PROGRESSION



TERRESTRIAL INTERFERENCE



SECURITY IMPACT

THESE ACTIVITIES ARE LINKED, MUTUALLY REINFORCING, AND SHARE INFRASTRUCTURE, PERSONNEL, AND INTENT.

7. CAPABILITY LIMITS & UNCERTAINTY



Reliability and accuracy remain unproven.



Resource constraints limit pace and sustainment.



Technological shortfalls require continued learning.



Intent, doctrine, and true capabilities are uncertain.

CAPABILITIES WILL EVOLVE—UNCERTAINTY IS ENDURING.

KEY TAKEAWAYS



DIRECT SECURITY RELEVANCE

North Korea's space and missile activities—and interference operations—pose real risks to regional security and stability.



AMBIGUITY MULTIPLIES RISK

Uncertainty about capabilities and intent complicates deterrence, crisis response, and escalation management.



DUAL-USE REALITY

The same technologies enable both space missions and long-range missile capabilities.



PERSISTENT MONITORING

Track launches, interference activity, technology trends, and supporting infrastructure continuously.



COOPERATION & RESILIENCE

Strengthen regional coordination, improve resilience to interference, and uphold responsible behavior in space and cyberspace.

INDIA AFTER MISSION SHAKTI: COUNTERSPACE CAPABILITIES AND LIMITS

FROM ASAT MILESTONE TO A DEVELOPING, LIMITED COUNTERSPACE POSTURE

MISSION SHAKTI: INDIA'S ASAT MILESTONE



On 27 March 2019, India conducted a direct-ascent anti-satellite (ASAT) test codenamed Mission Shakti.



A kinetically launched interceptor struck Microsat-R, a ~740 kg satellite, in low Earth orbit (~300 km).



This successful destructive ASAT test made India the fourth country to achieve this capability after the United States, Russia (USSR), and China.



WHY IT MATTERED

- ✓ Demonstrated reach, precision, and kill capability against an orbital target.
- ✓ Signaled India's arrival in the counterspace domain.
- ✓ Enhanced deterrence by holding space assets at risk.
- ✓ Also created space debris, underscoring the need for responsible behavior.

THE BROADER INDIAN PICTURE: BUILDING BLOCKS OF COUNTERSPACE CAPABILITY



SPACE SITUATIONAL AWARENESS (SSA)

- ISRO operates tracking networks and sensors.
- IN-SPACe is developing a national SSA system.
- Focus on cataloguing objects, conjunction warning, and anomaly detection.



MILITARY-SPACE ORGANIZATION

- Defence Space Agency (DSA) established in 2019 to integrate space into defence planning.
- Defence Space Research Organisation (DSRO) created in 2020 for defence space R&D.
- Tri-service commands are incorporating space capabilities.



ELECTRONIC WARFARE CONCERNS

- Reports of satellite signal spoofing and interference in the region.
- Vulnerability of GPS, navigation, and communication links is a growing concern.
- Investment in resilient communications and anti-jamming measures.



DIRECTED-ENERGY INTEREST

- DRDO has tested high-energy laser (HEL) systems against aerial targets.
- Potential future roles: dazzling sensors, disrupting optics, and defeating drones and satellites.
- Capability remains in early stages.



SPACE ASSET RESILIENCE

- India is expanding satellite capacity, redundancy, and ground infrastructure.
- Emphasis on protected links, hardened buses, and rapid recovery options.

COMPARISON PANEL: STRENGTHS, GROWTH AREAS, AND LIMITS

STRENGTHS



- Proven kinetic ASAT capability (Mission Shakti).
- Growing SSA architecture and sensor network.
- Dedicated military-space organizations (DSA, DSRO).
- Expanding satellite fleet for communications, imaging, navigation (NavIC).
- Strong R&D base and industry participation.



GROWTH AREAS

- Operational SSA with global coverage.
- Non-kinetic counterspace tools (EW, cyber, reversible capabilities).
- Directed-energy systems for space and ground roles.
- Space control doctrine, wargaming, and joint training.
- Resilience, hardening, and rapid reconstitution.



LIMITS

- Limited depth and diversity of counterspace toolkit.
- Fewer constellations and ISR assets than major powers.
- Limited global basing and persistent coverage.
- Early-stage directed-energy capability.
- Does not match the breadth and maturity of U.S., Russian, or Chinese counterspace portfolios.



INDIA SEEKS STRONGER MILITARY-SPACE CAPABILITIES BUT DOES NOT MATCH THE FULL BREADTH OF U.S., RUSSIAN, OR CHINESE COUNTERSPACE PORTFOLIOS.

TIMELINE: KEY MILESTONES SINCE MISSION SHAKTI



27 MARCH 2019
Mission Shakti
India conducts destructive ASAT test against Microsat-R.



AUGUST 2019
Creation of
Defence Space Agency (DSA)
to integrate space into defence.



2020
Establishment of
Defence Space Research
Organisation (DSRO)
for defence space R&D.



2021-2022
Progress on national
SSA system under
IN-SPACe; more sensors
and data sharing.



2023
Expansion of military
communications,
satellite capacity,
and protected links.



2024
Integration of space
capabilities in tri-service
doctrine and exercises
intensifies.



ONGOING
Focus on resilience,
non-kinetic tools,
directed energy,
and responsible
behavior in space.

KEY TAKEAWAYS



CREDIBLE DETERRENCE

Mission Shakti demonstrated reach and intent, enhancing deterrence by signaling that India can hold space assets at risk.



REGIONAL COMPETITION

Counterspace capabilities are advancing across the region. India must keep pace while managing escalation risks.



BUILD, INTEGRATE, RESILIENTLY

Sustained investment in SSA, non-kinetic tools, directed energy, doctrine, and resilient space systems is essential.



RESPONSIBLE BEHAVIOR IN SPACE

India should champion responsible, rule-based space behavior to ensure a secure and sustainable space environment.

EUROPE'S MILITARY SPACE RESPONSE: FRANCE, GERMANY, AND THE UNITED KINGDOM

STRENGTHENING ORGANIZATIONS, DOCTRINE, RESILIENCE, AND SPACE SITUATIONAL AWARENESS



WHY EUROPE IS TREATING SPACE AS A MORE CONTESTED DOMAIN



GROWING THREATS
Jamming, electronic attack, co-orbital activity, and anti-satellite weapons endanger space systems.



MISSION CRITICAL
Space underpins military communications, ISR, navigation, and missile warning—essential for national security.



VULNERABILITY & DEPENDENCY
Europe relies on space services that adversaries could disrupt, degrade, or deny.



STRATEGIC AUTONOMY
Stronger military-space capabilities increase resilience, deterrence, and decision-making independence.



GROWING ROLE IN MULTINATIONAL EXERCISES AND PARTNERSHIPS



ACTIVE IN MAJOR EXERCISES
Astral Knight, Pacific Skies, Olympic Defender, Steadfast Defender, and others.



COOPERATION FRAMEWORKS
NATO, EU (PESCO, EDF), EUSPA, ESA, and bilateral partnerships.



INFORMATION SHARING
Expanding space situational awareness data sharing and secure communications.



INDUSTRY & INNOVATION
Joint R&D, dual-use technologies, and resilient satellite architectures.

FRANCE	
 ORGANIZATION	- Commandement de l'Espace (CDE) – established 2019 - Part of French Space Command within the Air and Space Force
 DOCTRINE FOCUS	- Space as an operational domain - Space control and protection - Integrated space support to operations
 SSA & SURVEILLANCE	- GRAVES space surveillance radar - Optical sensors and military SSA network - Contributes to EU SST and NATO SSA
 ALLIANCES & PARTNERSHIPS	- Strong NATO and EU engagement - Bilateral cooperation with key allies - Support to European SST initiatives
 PRIORITIES	- Resilience of space systems - Deterrence and space control - Sovereign access and protection of assets

GERMANY	
 ORGANIZATION	- Das Weltraumkommando (Space Command) – established 2019 - Part of the German Air Force
 DOCTRINE FOCUS	- Space as a warfighting enabler and contested domain - Protection, support, and situational awareness - Whole-of-government approach
 SSA & SURVEILLANCE	- GESTRA military radar system - Optical telescopes and sensor upgrades - Active in EU SST Partnership and NATO SSA
 ALLIANCES & PARTNERSHIPS	- Deep NATO commitment - EU PESCO and EDF space projects - Strong ties with industry and allies
 PRIORITIES	- Resilient communications & PNT - SSA and early warning - Industrial base and innovation

THE UNITED KINGDOM	
 ORGANIZATION	- UK Space Command – established 2021 - Part of Air and Space Operations Centre (Royal Air Force)
 DOCTRINE FOCUS	- Integrated with Joint Operations - Space control, ISR, and protection - Enabling warfighting advantage
 SSA & SURVEILLANCE	- Flyingdales and other radar assets - Optical telescopes and SSA network - Key contributor to NATO and UK SSA
 ALLIANCES & PARTNERSHIPS	- Leading role in NATO space initiatives - Strong Five Eyes cooperation - Bilateral and industry partnerships
 PRIORITIES	- Resilience and protected services - Deterrence and space control - Innovation and rapid capability fielding

EUROPE'S MILITARY SPACE DEVELOPMENT TIMELINE	
2016+	Rising recognition of space as a military domain in Europe
2018–2019	France (2019) and Germany (2019) establish Space Commands
2021	United Kingdom establishes UK Space Command
2022+	EU Space Strategy for Security & Defence adopted
2023+	Increased investment in SSA, resilience, and secure services
2024+	More joint exercises and multinational capability development
2025+	Greater interoperability, data sharing, and deterrence posture

COMPARISON MATRIX: EUROPE'S MILITARY SPACE POSTURES				
DIMENSION	FRANCE	GERMANY	THE UNITED KINGDOM	
 MILITARY SPACE ORGANIZATION	Commandement de l'Espace (2019)	Das Weltraumkommando (2019)	UK Space Command (2021)	
 DOCTRINE EMPHASIS	Space as operational domain; control and protection	Space as warfighting enabler; protection and support	Integrated operations; space control and warfighting advantage	
 SSA & SURVEILLANCE	GRAVES radar; optical sensors; EU SST & NATO SSA	GESTRA radar; optical systems; EU SST & NATO SSA	Flyingdales radar; optical sensors; NATO & UK SSA	
 ALLIANCES & COOPERATION	NATO, EU, bilateral partnerships; European SST	NATO, EU (PESCO, EDF), industry and allied partnerships	NATO, Five Eyes, EU projects; industry partnerships	
 PRIORITY FOCUS	Resilience, deterrence, space control, sovereignty	Resilience, SSA, PNT, industrial & innovation	Resilience, deterrence, innovation, rapid capability	



EUROPE IS BUILDING STRONG, COMPLIMENTARY MILITARY SPACE CAPABILITIES that treat space as a contested and operational domain.



FRANCE, GERMANY, AND THE UNITED KINGDOM ARE INVESTING IN ORGANIZATIONS, DOCTRINE, SSA, AND RESILIENCE to protect critical space services.



COLLECTIVE SECURITY RELIES ON ALLIED COOPERATION, INFORMATION SHARING, and participation in exercises and joint projects.



DETERRENCE AND SPACE CONTROL CAPABILITIES ARE CENTRAL to preserving freedom of action in space.



CONTINUED COORDINATION AND INVESTMENT WILL DELIVER A MORE RESILIENT, INTEROPERABLE, AND DETERRENT EUROPE.

THE NUCLEAR ASAT THREAT: WHY A SINGLE DETONATION COULD IMPERIL LOW EARTH ORBIT

A NUCLEAR BLAST IN SPACE OR THE UPPER ATMOSPHERE CREATES ELECTROMAGNETIC AND RADIATION EFFECTS THAT CAN DISRUPT OR DAMAGE SATELLITES AND INFRASTRUCTURE ACROSS VAST AREAS—NOT JUST A SINGLE TARGET.

WHY NUCLEAR IS DIFFERENT

Unlike conventional ASAT weapons that produce localized debris, a nuclear detonation releases energy in forms that propagate over thousands of kilometers, affecting many satellites and systems at once.



- ✓ No need for a direct hit on each satellite
- ✓ Effects scale with altitude and yield
- ✓ Impacts electronics, not just physical structures
- ✓ Hard to shield against across entire constellations

EMP EFFECTS



A nuclear burst generates a powerful electromagnetic pulse (EMP) that can couple into spacecraft and ground systems.

- **Fast EMP:** disrupts or damages satellite electronics and onboard computers
- **Intermediate EMP:** induces currents in cables, antennas, and components
- **Long-duration EMP:** can overload power grids and disrupt communications over wide areas



EMP effects increase with altitude and line of sight—impacting satellites beyond the blast point and even ground infrastructure.

RADIATION EFFECTS



Nuclear detonation produces intense x-rays, gamma rays, and energetic particles that can damage or degrade electronics and solar cells.

- **Total ionizing dose:** degrades microelectronics and solar panels
- **Single-event effects:** glitches, memory upsets, and unintended resets
- **Charging and discharging:** can cause arcing and permanent failure



Radiation can affect satellites regardless of orientation and can accumulate over time, causing delayed failures.

DISRUPTION TO SATELLITES AND GROUND INFRASTRUCTURE



Satellites: loss of control, degraded sensors, communications blackout, or permanent failure across many platforms.



Ground Stations: EMP can damage receivers, antennas, and servers; disrupt command and control links.



Power Grids: geomagnetically induced currents from EMP can cause voltage surges, equipment damage, and outages.



Communications Networks: widespread service interruptions and data loss.

WIDE-AREA CONSEQUENCES



NAVIGATION & TIMING

Disruption to GNSS and satellite timing affects transportation, banking, telecom, and power systems.



WEATHER & EARTH OBSERVATION

Loss of data from weather, climate, and disaster monitoring satellites reduces forecasting and emergency response.



COMMUNICATIONS

Outages to TV, radio, broadband, and military communications across large regions.



TRANSPORTATION

Aviation, maritime, and rail operations face navigation and communication disruptions.



ECONOMY & SOCIETY

Financial systems, supply chains, emergency services, and daily life all depend on reliable space and ground systems.



THE EFFECTS ARE NOT LOCALIZED. THEY CAN SPREAD ACROSS CONTINENTS AND AFFECT BILLIONS OF PEOPLE.

WHY ONE DETONATION CAN ENDANGER MANY SATELLITES

- ✓ EMP and radiation propagate outward in all directions.
- ✓ Higher-altitude bursts have a larger footprint.
- ✓ Satellites share similar orbits and altitude bands.
- ✓ Modern constellations have many satellites—more targets in range.
- ✓ Cascading failures can compound disruption over time.



THE CONSEQUENCE CHAIN

DETONATION



Nuclear device detonates in space or the upper atmosphere.

RADIATION / EMP EFFECTS



Powerful radiation and EMP spread over a wide area, affecting satellites and ground systems.

SATELLITE DISRUPTION



Electronics degrade or fail, communications lost, navigation degraded, data disrupted.

BROADER IMPACTS



Services disrupted, economies hit, security weakened, society affected.

STRATEGIC INSTABILITY & TREATY CONCERNS



Attribution challenges: effects can be misread, raising the risk of escalation.



Crisis instability: leaders may face pressure to respond to uncertain or ambiguous events.



Arms race risk: incentives to build or deploy similar capabilities for “deterrence.”



Treaty concerns: a nuclear ASAT capability would undermine the Outer Space Treaty's peaceful use principle and global norms.



OPEN-SOURCE CONCERNS ABOUT A POTENTIAL RUSSIAN CONCEPT

Open-source reporting has raised concerns about a Russian space-based capability that could deliver a nuclear device for use against satellites. Details remain unconfirmed, and no public evidence shows deployment.

THE RISK STEMS FROM THE POSSIBILITY, NOT JUST THE PROOF.

KEY TAKEAWAYS

- ✓ A nuclear detonation in space is not just an attack on one satellite.
- ✓ It is an attack on the shared orbital environment.
- ✓ The consequences can be global, long-lasting, and hard to reverse.
- ✓ Protecting space is essential to protecting modern society.

WHAT TO WATCH IN COUNTERSPACE: TRENDS SHAPING THE NEXT DECADE

THE FUTURE IS LIKELY MORE CROWDED, CONTESTED, COMPETITIVE, AND OPERATIONALLY IMPORTANT

MAJOR TRENDS TO WATCH

1 PROLIFERATION OF CAPABILITIES



More states and non-state actors pursue counterspace capabilities across all domains.

2 MORE DUAL-USE SYSTEMS



Civil, commercial, and military uses blur, complicating attribution and response.

3 AUTONOMOUS & AI-ENABLED OPERATIONS



AI, autonomy, and advanced analytics enable faster decision-making and more complex operations.

4 GROWTH OF COMMERCIAL PARTICIPATION



Commercial providers expand launch, data, connectivity, and services—driving access and risk.

5 RESILIENCE & PROLIFERATED ARCHITECTURES



Distributed systems, many small satellites, and rapid replaceability strengthen survivability and continuity.

6 TIGHTER LINKS BETWEEN CYBER AND SPACE



Cyber operations increasingly target or support space systems—and vice versa.

7 CONTINUED RPO AMBIGUITY



Norms, laws, and thresholds remain unclear, creating ambiguity and risk of escalation.

8 COMPETITION OVER NORMS & BEHAVIOR



States compete to shape norms and legitimacy around responsible behavior in space.

9 RISING IMPORTANCE OF ALLIED COORDINATION



Allied and partner coordination is essential to deter, respond, and sustain shared interests.

WHAT STATES AND OPERATORS SHOULD PREPARE FOR



PERSISTENT, MULTI-DOMAIN THREATS

Expect coordinated actions—kinetic and non-kinetic—across space, cyber, electronic, and information domains.



GREATER CONGESTION AND INTERDEPENDENCE

More actors and assets increase collision risk and create cascading vulnerabilities across critical services.



SHORTER WARNING TIMES

Advanced sensors, AI, and automation compress decision cycles for attack and defense.



GREY ZONE AND AMBIGUOUS ACTS

Sub-threshold and reversible actions will be used to signal, coerce, or degrade without clear attribution.



SUPPLY CHAIN AND TECHNOLOGY RISKS

Dependencies on launch, components, data, and software create exposure points.



ECONOMIC AND SOCIETAL IMPACTS

Disruption to space services can quickly affect economies, security, and public trust.



COUNTERSPACE COMPETITION IS ACCELERATING.

PREPARE.
DETER.
RESILIENTLY OPERATE.
RESPONSIBLY LEAD.



WHAT MAY CHANGE FASTEST



1 AI & AUTONOMY

Rapid advances will outpace policies and defensive adaptations.



2 COMMERCIAL LAUNCH & LEO CONSTELLATIONS

Lower costs, higher cadence, and larger constellations will transform access and target sets.



3 CYBER CAPABILITIES

Offensive capabilities and cross-domain exploitation will expand quickly.



4 SENSING & DATA ADVANTAGE

Persistent sensing and data fusion will improve attribution and targeting.



5 NORMS & RULEMAKING

Norms, rules, and expectations may solidify—or fragment—based on action and leadership.

TREND IMPACT & UNCERTAINTY MATRIX

IMPACT: ● Low ● Medium ● High ● Very High UNCERTAINTY: ● Low ● Medium ● High

	IMPACT				UNCERTAINTY		
	Low	Medium	High	Very High	Low	Medium	High
Proliferation of Capabilities							
More Dual-Use Systems							
Autonomous & AI-Enabled Operations							
Growth of Commercial Participation							
Resilience & Proliferated Architectures							
Tighter Links: Cyber and Space							
Continued RPO Ambiguity							
Competition Over Norms & Behavior							
Rising Importance of Allied Coordination							

KEY TAKEAWAYS



PREPAREDNESS

Invest in people, data, and capabilities. Train, exercise, and plan for multi-domain counterspace scenarios.



RESILIENCE

Design for survivability: diversity, distribution, redundancy, and rapid reconstitution.



TRANSPARENCY & RESPONSIBILITY

Promote norms, share information, and act responsibly to reduce risk and build trust.



DETERRENCE THROUGH STRENGTH & UNITY

Credible capabilities, clear resolve, and allied coordination deter aggression and protect shared interests.

COUNTERSPACE CAPABILITIES 101 GLOSSARY

A GLOSSARY OF KEY TERMS, CONCEPTS, AND DEFINITIONS FOR COUNTERSPACE, SPACE SECURITY, AND MILITARY SPACE OPERATIONS.



WEAPONS AND EFFECTS

Understand counterspace weapons, mechanisms, and their intended effects on space capabilities.



ORBITS AND ARCHITECTURES

Explore orbital regimes, system architectures, and the space assets they enable.



SITUATIONAL AWARENESS AND TRACKING

Learn the sensors, data, and processes used to detect, track, and assess objects in space.



CYBER AND ELECTRONIC WARFARE

Examine cyber, electronic, and informational capabilities that affect space systems.



POLICY AND RESILIENCE

Review policies, norms, and resilience strategies that protect space capabilities and services.



This glossary provides a common language for understanding the critical concepts, systems, threats, and operations that shape counterspace activity and space security. Clear terms build stronger understanding, better decisions, and more resilient space capabilities.

COUNTERSPACE WEAPONS AND EFFECTS

A GLOSSARY OF KEY TERMS AND THEIR EFFECTS

Counterspace weapons are systems or capabilities designed to disrupt, degrade, deny, deceive, damage, or destroy space assets and the services they provide. They can act from the ground, air, sea, or space, and may use kinetic or non-kinetic means. Understanding the weapons, methods, and effects is essential for assessing risk and protecting space capabilities.

TERM	DEFINITION
 ANTI-SATELLITE WEAPON (ASAT)	Any weapon or capability designed to hold at risk, disrupt, degrade, deny, deceive, damage, or destroy space systems.
 DIRECT-ASCENT ASAT	A missile launched from the Earth's surface that travels directly (or near-directly) to a space target to disable or destroy it.
 CO-ORBITAL ASAT	A spacecraft placed into orbit that approaches, interferes with, or attacks another space object through proximity operations or by other means.
 KINETIC EFFECT	An effect produced by physical impact or physical force, such as collisions, fragments, or other physical destruction.
 NON-KINETIC EFFECT	An effect achieved without physical impact, such as through energy, signals, information, or cyber means.
 HARD KILL	An action that physically destroys, disables, or renders a space asset inoperable, often producing debris.
 SOFT KILL	An action that disrupts, degrades, or interferes with a space asset or its operations without physically destroying it.
 DIRECTED ENERGY	The use of focused energy (such as lasers or high-power microwaves) to dazzle, heat, damage, or disrupt sensors or electronics.
 JAMMING	The intentional transmission of radio frequency energy to interfere with or block legitimate communications or links.
 SPOOFING	The transmission of deceptive signals to mislead a satellite about timing, position, or other data, causing it to produce errors.
 CYBERATTACK	The use of malicious digital activity to disrupt, degrade, or take control of space systems, networks, or ground segment operations.
 REVERSIBLE VS. IRREVERSIBLE EFFECTS	Reversible effects are temporary and can be undone or recovered from. Irreversible effects cause lasting damage, destruction, or long-term loss.

EFFECTS COMPARISON		
	 DESTRUCTIVE	 NON-DESTRUCTIVE
 TEMPORARY (EFFECT DURATION)	TEMPORARILY DESTRUCTIVE Causes physical damage that may be repairable; recovery or replacement is possible. Example: a satellite survives but needs repairs.	TEMPORARILY NON-DESTRUCTIVE Disrupts or degrades operations for a period of time without causing physical damage. Example: temporary jamming of communications.
 PERMANENT (EFFECT DURATION)	PERMANENTLY DESTRUCTIVE Causes lasting destruction or removes the asset from use, often creating debris. Example: direct-ascent ASAT destroys a satellite.	PERMANENTLY NON-DESTRUCTIVE Causes lasting degradation or impairment without physical destruction; recovery may be impractical or impossible. Example: long-term data corruption via cyberattack.

KEY TAKEAWAYS	
	COUNTERSPACE TOOLS CAN DISRUPT, DEGRADE, DENY, DECEIVE, DAMAGE, OR DESTROY SPACE CAPABILITIES AND THE SERVICES THEY PROVIDE.
	EFFECTS RANGE FROM SUBTLE TO SEVERE, AND CAN BE TEMPORARY OR PERMANENT.
	MANY COUNTERSPACE CAPABILITIES ARE DUAL-USE, MEANING THEY CAN SERVE BOTH CIVIL AND MILITARY PURPOSES.
	ATTRIBUTION IS OFTEN CHALLENGING DUE TO PROXIES, PLAUSIBLE DENIABILITY, AND COMPLEX TECHNIQUES.

ORBITS AND SPACE ARCHITECTURES

A GLOSSARY OF KEY TERMS FOR ORBITAL REGIONS AND SYSTEM DESIGN

Space architecture describes how satellites, ground systems, and orbital choices are organized to deliver missions. Understanding orbital regions, system components, and architectural approaches is essential for designing capable, resilient, and cost-effective space systems.

TERM	DEFINITION
 LEO (LOW EARTH ORBIT)	An orbital region close to Earth that enables low latency, high data rates, and frequent revisits.
 MEO (MEDIUM EARTH ORBIT)	A mid-altitude orbital region that offers a balance of coverage, latency, and constellation size.
 GEO (GEOSTATIONARY ORBIT)	An orbital region above the equator where satellites appear fixed over one point on Earth, providing continuous coverage.
 HEO (HIGHLY ELLIPTICAL ORBIT)	Elliptical orbits with high apogee that provide long dwell times over targeted regions.
 CISLUNAR SPACE	The space region around the Moon and between Earth and the Moon, used for exploration, staging, and communication.
 CONSTELLATION	A coordinated network of multiple satellites working together to provide global or regional service.
 PROLIFERATED LEO	A large number of small satellites in LEO that increase capacity, coverage, and redundancy.
 SATELLITE BUS	The satellite platform that provides power, propulsion, attitude control, communications, and other core functions.
 PAYLOAD	The mission-specific instruments or equipment that perform the primary mission objectives.
 GROUND SEGMENT	The network of ground stations, control centers, and software that operate, control, and communicate with satellites.
 DISAGGREGATION	Breaking capabilities into smaller, modular functions distributed across multiple assets.
 RECONSTITUTION	Reassembling distributed functions through the network to deliver coherent mission outcomes.

COMMON ORBITAL REGIONS: AT-A-GLANCE		
ORBITAL REGION	GENERAL CHARACTERISTICS	TYPICAL MISSION USES
 LEO	Close to Earth; low latency; requires more satellites for continuous coverage.	Earth observation, communications, IoT, scientific missions.
 MEO	Moderate altitude; balanced latency and coverage; smaller constellations than LEO.	Navigation, timing, regional communications.
 GEO	Fixed over one location; continuous coverage of a broad region.	Broadcast, enterprise communications, weather, disaster response.
 HEO	Long dwell over high-latitude or targeted areas; variable latency.	Global communications, surveillance, specialized missions.
 CISLUNAR SPACE	Beyond Earth's immediate environment; greater distances and dynamics.	Lunar exploration, deep space staging, communications relay.

KEY TAKEAWAYS	
	ORBIT CHOICE DRIVES COVERAGE AND ACCESS: Each region offers different trade-offs in reach, revisit, and service continuity.
	LATENCY AND PERSISTENCE VARY BY ORBIT: Lower orbits enable low latency and high data rates; higher orbits provide larger areas of continuous access.
	VULNERABILITY DEPENDS ON ARCHITECTURE: Orbit and system design affect exposure to threats, interference, and environmental risks.
	RESILIENCE COMES FROM DESIGN: Layered orbits, disaggregation, and reconstitution create adaptable and survivable mission capabilities.

SPACE SITUATIONAL AWARENESS AND TRACKING

A GLOSSARY OF KEY TERMS FOR DETECTING, TRACKING, AND CHARACTERIZING OBJECTS IN SPACE

Space situational awareness (SSA), also called space domain awareness (SDA), is the ability to detect, track, characterize, and understand objects in space and the environment in which they operate. It supports safe operations, collision avoidance, space traffic management, and protection of space assets and services.

TERM	DEFINITION
 SSA OR SDA	Space Situational Awareness or Space Domain Awareness; understanding objects in space and their environment to enable safe and secure operations.
 CATALOG	A database of known space objects with identifiers, orbits, and other parameters used for analysis and operations.
 SURVEILLANCE	Systematic search and monitoring of space to detect and monitor objects of interest.
 TRACKING	Continuous measurements of an object's position and velocity to maintain and refine its predicted orbit.
 SENSOR	Any instrument or system that detects objects or environment data, including radar, optical, and space-based sensors.
 RADAR	Radio wave systems that detect, range, and track objects day or night and through clouds.
 OPTICAL TELESCOPE	Telescopes that use visible and infrared light to detect and measure objects, providing high accuracy and characterization.
 CONJUNCTION	A predicted close approach between two or more objects in space within a defined time and distance threshold.
 CONJUNCTION ASSESSMENT	Analysis of a conjunction to estimate collision probability and determine necessary mitigation actions.
 EPHEMERIS	A set of time-tagged position and velocity data that predicts an object's future trajectory.
 CHARACTERIZATION	Determining physical and behavioral properties of objects, such as size, shape, rotation, material, and function.
 ATTRIBUTION	Assessing the likely owner or source of an object based on technical, behavioral, or contextual evidence.
 SPACE WEATHER	Conditions in space driven by the Sun that can affect satellites, communications, GPS, and other space-based systems.

THE SSA PROCESS: DETECT → TRACK → ASSESS → WARN



DETECT

Sensors scan space to find new and known objects.



TRACK

Measure positions and velocities to maintain accurate object tracks.



ASSESS

Evaluate risks and impacts, including conjunction and threat assessment.



WARN

Issue timely alerts and advisories to enable action and mitigate risk.



KEY TAKEAWAYS



AWARENESS STARTS WITH SENSORS: Diverse sensors—on the ground and in space—detect and observe objects and the space environment.



DATA FUSION DRIVES ACCURACY: Combining data from many sources improves tracking precision and reduces uncertainty.



PREDICTION ENABLES SAFETY: Accurate orbits and models support conjunction assessment and informed decision-making.



TIMELY WARNING PROTECTS OPERATIONS: Early alerts and clear information enable effective mitigation and mission assurance.

RENDEZVOUS, PROXIMITY, AND ON-ORBIT OPERATIONS

A GLOSSARY OF KEY TERMS FOR CLOSE APPROACHES, SERVICING, AND DUAL-USE ACTIVITIES

Rendezvous and proximity operations enable satellites to approach, observe, attach to, or interact with other objects in space. These same capabilities can support beneficial activities such as servicing and repair—or enable harmful actions such as interference or attack. Clear terminology helps promote transparency, responsible behavior, and informed risk assessment.

TERM	DEFINITION
 RPO	Rendezvous and Proximity Operations. Activities in which a spacecraft changes its position or velocity to approach, operate near, or interact with another space object.
 RENDEZVOUS	Maneuvers to reduce the relative distance to another object with the intention of arriving at a specified location or point for operations.
 PROXIMITY OPERATIONS	Operating near another object within a close distance envelope without docking or physical contact. Includes observation, imaging, or monitoring.
 STATION-KEEPING	Maneuvers to maintain position and orientation relative to another object or point in space, typically within a defined tolerance.
 DOCKING	Creating a rigid mechanical connection between two spacecraft to allow power, data, or crew transfer.
 BERTHING	Securing to a pre-installed fixture or capture point on a host object, usually designed for repeatable visits or long-duration attachment.
 INSPECTION SATELLITE	A spacecraft designed or used to observe, image, or collect data about another object to assess its condition, characteristics, or behavior.
 BODYGUARD SATELLITE	A spacecraft that accompanies, positions near, or monitors another object to provide protection, deterrence, or responsive options.
 ON-ORBIT SERVICING	Activities that maintain, repair, upgrade, or extend the life of another object in space to preserve or enhance its functionality.
 REFUELING	Transfer of propellant from one spacecraft to another to restore or increase its maneuver capability or extend mission life.
 GRAPPLING	Capturing or restraining an object using robotic arms, nets, harpoons, or other capture mechanisms.
 DEBRIS REMOVAL	Capturing, deorbiting, or relocating defunct or fragmented objects to reduce collision risk and environmental hazards.
 DUAL-USE TECHNOLOGY	Technologies, systems, or techniques that have legitimate civil or commercial applications but can also be used for military or harmful purposes.

WHY THESE ACTIVITIES MATTER



SUPPORT SERVICING AND SUSTAINABILITY

Enable inspection, repair, refueling, and life extension that enhance reliability and reduce space debris.



ENABLE INSPECTION AND AWARENESS

Allow collection of information about other objects to support domain awareness, verification, and risk assessment.



PROVIDE DEFENSIVE OPTIONS

Support protection of critical assets through presence, monitoring, and the ability to respond to threats.



POSE OFFENSIVE RISKS

The same capabilities can be used to interfere with, degrade, disable, capture, or destroy other objects.

KEY TAKEAWAYS



AMBIGUITY IS INHERENT. Many close approaches and capabilities can be interpreted in multiple ways.



MANEUVERABILITY IS POWER. Control of position and proximity creates options that can be benign or malign.



OPERATOR INTENT MATTERS. The purpose and context behind an operation determine whether it is responsible or threatening.



CONTEXT IS CRITICAL. Understanding history, behavior, communications, and transparency is essential for sound assessment.

PNT, GNSS, AND ELECTRONIC WARFARE

A GLOSSARY OF KEY TERMS FOR NAVIGATION SIGNALS, INTERFERENCE, AND DENIAL

Global navigation signals enable positioning, timing, and communication for military, civilian, and critical infrastructure systems. Adversaries can disrupt, deceive, or deny these signals to degrade operations and decision-making. Understanding key terms helps organizations assess risk, build resilience, and respond effectively.

TERM	DEFINITION
 PNT	Positioning, Navigation, and Timing. The combination of capabilities that determine location, provide direction or course, and establish precise time.
 GNSS	Global Navigation Satellite System. A network of satellites that broadcast signals enabling global positioning, navigation, and timing.
 GPS	Global Positioning System. The U.S. GNSS operated by the U.S. Space Force that provides global PNT services.
 SIGNAL INTEGRITY	The trustworthiness of a signal, including accuracy, continuity, and authenticity. High integrity means users can rely on the information provided.
 JAMMING	The intentional transmission of radio energy to block or degrade legitimate navigation signals.
 SPOOFING	The transmission of fake navigation signals to mislead receivers about position, time, or velocity.
 MEACONING	The rebroadcast of genuine navigation signals, intentionally delayed or altered, to mislead receivers.
 INTERFERENCE	Any unwanted signal or noise that degrades the quality, availability, or usability of navigation signals.
 UPLINK	The transmission path from a ground station to a satellite. Used to send commands or data.
 DOWNLINK	The transmission path from a satellite to a receiver on or near the Earth. Used to broadcast navigation signals.
 NAVIGATION WARFARE	Military actions to exploit, attack, protect, or deny an adversary's use of PNT capabilities while ensuring friendly access.
 ELECTRONIC WARFARE	The use of electromagnetic energy to control the electromagnetic spectrum or attack an enemy. Includes electronic attack, protection, and support.

EFFECTS COMPARISON		
 JAMMING	 SPOOFING	 MEACONING
Like shouting so loudly that the real signal is drowned out. Receivers may lose lock or experience large errors.	Like giving a fake address to send someone the wrong way. Receivers believe the false signal and navigate based on incorrect information.	Like echoing a true signal with a delay or change. Receivers are misled because the signal arrives late or from the wrong time.

KEY TAKEAWAYS
 PNT SIGNALS CAN BE DISRUPTED, DECEIVED, OR DENIED THROUGH JAMMING, SPOOFING, AND MEACONING.
 THESE EFFECTS CAN BE TEMPORARY OR PERSISTENT AND MAY VARY IN INTENSITY AND IMPACT.
 IMPACTS CAN AFFECT TIMING, NAVIGATION, AND COMMUNICATIONS ACROSS MILITARY AND CIVILIAN SYSTEMS.
 RESILIENCE REQUIRES AWARENESS, REDUNDANCY, MONITORING, AND RAPID RESPONSE.

CYBER AND GROUND-SEGMENT SECURITY

A GLOSSARY OF KEY TERMS FOR DIGITAL RISK, COMMAND LINKS, AND SUPPORTING INFRASTRUCTURE

Cyber and ground-segment security protects the networks, systems, and data that control and support space missions. Threats can target ground stations, command links, and supporting infrastructure to steal data, disrupt operations, or deny mission services. Understanding these terms helps build resilient systems and maintain trust, availability, and mission success.

TERM	DEFINITION
 GROUND SEGMENT	The Earth-based systems and networks that communicate with, control, and support spacecraft and missions.
 TT&C (TELEMETRY, TRACKING & COMMAND)	Functions that provide telemetry data downlink, tracking of the spacecraft, and command uplink to operate and manage the spacecraft.
 COMMAND UPLINK	The transmission of commands from ground systems to a spacecraft to control its behavior and payload operations.
 TELEMETRY	Data sent from a spacecraft to the ground that reports system health, status, and mission performance.
 AUTHENTICATION	Verifying the identity of users, systems, or devices before allowing access to networks or resources.
 ENCRYPTION	The process of encoding data to protect its confidentiality and integrity during storage and transmission.
 INTRUSION	Unauthorized access or activity within a system or network.
 MALWARE	Malicious software designed to infiltrate, damage, disrupt, or gain unauthorized access to systems.
 RANSOMWARE	Malware that locks or encrypts systems or data and demands payment for restoration or decryption.
 SUPPLY CHAIN ATTACK	An attack that targets trusted suppliers or third-party components to compromise downstream systems.
 DENIAL OF SERVICE	An attack that overwhelms or degrades systems or networks to make services unavailable to users.
 SEGMENTATION	Separating networks or systems into segments to limit exposure and contain potential threats.
 PATCHING	Applying updates or fixes to software and systems to close vulnerabilities and improve security.

HOW CYBER RISK CAN AFFECT YOUR MISSION



KEY TAKEAWAYS

-  **SPACE MISSIONS RELY ON SOFTWARE, NETWORKS, AND HUMAN OPERATORS AS MUCH AS ON HARDWARE.**
-  **STRONG AUTHENTICATION, ENCRYPTION, AND NETWORK SEGMENTATION REDUCE THE ATTACK SURFACE.**
-  **MAINTAIN VIGILANCE ACROSS THE SUPPLY CHAIN, SYSTEM LIFECYCLE, AND OPERATIONAL ENVIRONMENT.**
-  **CONTINUOUS MONITORING, PATCHING, AND INCIDENT RESPONSE ARE ESSENTIAL FOR MISSION RESILIENCE.**

MILITARY SPACE, ISR, AND COMMAND

A GLOSSARY OF KEY TERMS FOR SPACE-ENABLED OPERATIONS AND DECISION SUPPORT

Military space capabilities extend national power by providing persistent awareness, secure communications, and precise timing. These systems enable commanders to sense, understand, decide, and act—faster and more effectively—across any domain.

TERM	DEFINITION
 ISR	Intelligence, Surveillance, and Reconnaissance. The integrated activities and capabilities used to collect, process, and disseminate information for operations.
 RECONNAISSANCE	The active collection of information about enemy forces or areas of interest, typically using sensors or other detection methods.
 SURVEILLANCE	The persistent observation and monitoring of areas, forces, or activities to detect changes and track developments over time.
 MISSILE WARNING	Detection and alerting of missile launches or threats using space-based sensors to provide early warning of potential attacks.
 MISSILE TRACKING	Monitoring and determining the location, trajectory, and status of missiles to support defense and response operations.
 SATCOM	Satellite Communications. The use of space-based systems to provide voice, data, and video communications worldwide.
 COMMAND AND CONTROL	The exercise of authority and direction by a commander over assigned and attached forces in the accomplishment of the mission.
 BATTLE MANAGEMENT	The process of integrating ISR, fires, mobility, and sustainment to create, maintain, and exploit a common operational picture.
 KILL CHAIN	The sequence of steps from detecting a target to assessing the outcome of an engagement.
 TARGETING	The process of selecting and prioritizing targets and matching the appropriate response to achieve mission objectives.
 EARLY WARNING	Timely detection of threats or events to provide decision advantage and allow for proactive response.
 JOINT OPERATIONS	Operations conducted by forces from two or more military Services, or in coordination with allies and partners, to achieve unity of effort.

HOW SPACE SYSTEMS SUPPORT OPERATIONS



AWARENESS

Space-based sensors provide wide-area, persistent observation and early warning to see first and understand the environment.



COMMUNICATION

Satellites deliver secure, resilient communications that connect forces, partners, and decision-makers anytime, anywhere.



DECISION-MAKING

Timely information and shared understanding enable commanders to plan, act, and adapt with speed and precision.

KEY TAKEAWAYS



INTEGRATION MULTIPLIES EFFECTIVENESS.

Combining ISR, SATCOM, and command capabilities enables unified, synchronized operations.



TIMING CREATES ADVANTAGE.

Speed of detection, decision, and action is critical across the kill chain.



INFORMATION FLOW IS THE LIFELINE.

Accurate, secure, and shared data drives understanding and effective action.



DEPENDENCE ON SPACE SERVICES IS REAL.

Protect, defend, and responsibly use space to ensure mission success and national security.

ORBITAL DEBRIS AND NUCLEAR EFFECTS

A GLOSSARY OF KEY TERMS FOR SPACE ENVIRONMENT HAZARDS AND WIDE-AREA EFFECTS

Space operations rely on a safe and stable environment. Human activities can create debris that endangers spacecraft and can also introduce nuclear-related hazards that produce wide-area effects. Understanding these terms helps operators, planners, and policymakers assess risk, protect assets, and support responsible decision-making.

TERM	DEFINITION
 ORBITAL DEBRIS	Human-made objects and fragments in orbit that no longer serve a useful function. Debris ranges from large, trackable objects to tiny particles traveling at high speeds.
 FRAGMENTATION	The breaking of an object into multiple pieces due to an impact, explosion, or other event, creating additional debris.
 CONJUNCTION RISK	The probability that two objects in orbit will come close enough in space and time for a collision to occur.
 COLLISION AVOIDANCE	Actions taken to reduce the risk of a collision, such as tracking, analysis, maneuvering, or design measures.
 DEBRIS FIELD	A region in orbit containing a higher concentration of debris, often resulting from a fragmentation event.
 LONG-LIVED DEBRIS	Debris that remains in orbit for extended periods due to altitude, low atmospheric drag, or orbital characteristics.
 KESSLER SYNDROME	A theoretical cascade of collisions where increasing debris creates more collisions, potentially making certain orbits unusable.
 HIGH-ALTITUDE NUCLEAR DETONATION	The explosion of a nuclear device in space or high in the atmosphere, producing wide-area effects without surface impact.
 ELECTROMAGNETIC PULSE	A burst of electromagnetic energy from a nuclear detonation that can disrupt or damage electronics over large distances.
 RADIATION BELT ENHANCEMENT	Disturbances that increase the intensity or extent of natural radiation belts, raising exposure risks for spacecraft and electronics.
 CONTAMINATION	The spread of radioactive particles or debris from a detonation that can contaminate spacecraft surfaces and sensors.
 COLLATERAL EFFECTS	Unintended consequences to space assets, services, and operations not intended as direct targets, including widespread and long-duration impacts.

DEBRIS HAZARDS VS. NUCLEAR-RELATED SPACE HAZARDS			
	DEBRIS HAZARDS	VS.	 NUCLEAR-RELATED SPACE HAZARDS
	Arise from collisions, fragmentations, and other physical events.		Result from nuclear detonations in space or high in the atmosphere.
	Primarily threaten spacecraft through impact and cumulative risk.		Cause wide-area effects through EM pulse, radiation, and contamination.
	Effects can persist for decades or longer in orbit.		Effects can be immediate and wide-reaching, with long-term environmental impacts.
	Risk grows with more debris and repeated events.		Consequences can extend beyond space to systems and services on Earth.
KEY TAKEAWAYS			
	PERSISTENCE: Debris and nuclear-related effects can remain for long periods, creating ongoing risks to current and future operations.		
	WIDE-AREA IMPACT: Hazards can affect multiple orbits, many assets, and essential services across large regions.		
	UNPREDICTABILITY: Events can occur without warning and have uncertain severity and duration.		
	LONG-TERM CONSEQUENCES: The environmental and operational impacts can outlast the initial event and be difficult and costly to reverse.		

POLICY, NORMS, DETERRENCE, AND RESILIENCE

A GLOSSARY OF KEY TERMS FOR GOVERNANCE, RISK REDUCTION, AND MISSION CONTINUITY

Sustainable space operations rely on clear policies, shared norms, credible deterrence, and strong resilience. Together, they help prevent harmful behavior, manage risk, respond to incidents, and ensure missions can continue. Understanding these terms enables better decisions, stronger cooperation, and a more stable and secure space environment.

TERM	DEFINITION
 POLICY	Official statements of intent and principles that guide decisions, priorities, and actions for space activities.
 DOCTRINE	Fundamental strategies and operating principles that describe how forces and systems are organized and employed.
 NORM	Widely accepted expectations of responsible behavior that help prevent harmful actions and build trust.
 TRANSPARENCY	Sharing relevant information about capabilities, activities, and intentions to reduce uncertainty and misinterpretation.
 CONFIDENCE-BUILDING MEASURE	Voluntary actions—such as notifications, data sharing, or observer programs—that reduce risk and strengthen mutual confidence.
 DETERRENCE	Discouraging harmful actions by convincing potential adversaries that costs will outweigh any possible gains.
 RULES OF ENGAGEMENT	Pre-established guidance that defines when and how force or other responses may be used.
 ESCALATION MANAGEMENT	Actions and communication intended to prevent, halt, or reverse cycles of escalating competition or conflict.
 RESILIENCE	The ability to anticipate, withstand, adapt to, and recover from disruptions while continuing mission-essential functions.
 REDUNDANCY	Using backups, diversity, and extra capacity in systems and processes to reduce the impact of failures or attacks.
 MISSION ASSURANCE	Planned activities and controls that protect systems and data, reduce risk, and support the reliable execution of missions.
 RECONSTITUTION	Restoring degraded capabilities and services to full effectiveness after a disruption or attack.

HOW THEY DIFFER—AND WORK TOGETHER



NORMS

SHAPE EXPECTATIONS.

Norms define what responsible behavior looks like. They build trust, reduce uncertainty, and lower the chance of harmful actions.



DETERRENCE

DISCOURAGES HARM.

Deterrence convinces potential adversaries that aggression will fail or impose unacceptable costs, making harmful actions less likely.



RESILIENCE

ENDURES AND RECOVERS.

Resilience ensures missions can withstand disruptions, adapt to change, and recover quickly, limiting long-term impact.



KEY TAKEAWAYS



PREVENTION FIRST: Policies, norms, and transparency reduce risk and prevent crises before they start.



SIGNAL CLEARLY: Deterrence and rules of engagement communicate resolve and reduce miscalculation.



RECOVER STRONGLY: Resilience, redundancy, and reconstitution enable rapid recovery and mission continuity.



SUSTAIN STABILITY: When these elements work together, they create a safer, more predictable, and more stable space environment.

COUNTERSPACE CAPABILITIES 101



PRIMARY SOURCE REFERENCE



GLOBAL COUNTERSPACE CAPABILITIES: AN OPEN SOURCE ASSESSMENT



SECURE WORLD FOUNDATION • 2026



A COUNTRY-BY-COUNTRY OPEN-SOURCE ASSESSMENT OF COUNTERSPACE CAPABILITIES, INCLUDING DIRECT-ASCENT ASAT, CO-ORBITAL SYSTEMS, ELECTRONIC WARFARE, DIRECTED ENERGY, CYBER, POLICY, DOCTRINE, AND SPACE SECURITY TRENDS.



OFFICIAL ONLINE LOCATION

<https://www.swfound.org/publications-and-reports/2026-global-counterspace-capabilities-report>



SERIES COVERAGE

- GLOBAL LANDSCAPE
- TECHNOLOGY AND DOCTRINE
- REGIONAL POWERS
- EMERGING THREATS



KEY THEMES DRAWN FROM THE SOURCE

- ANTI-SATELLITE WEAPONS
- ELECTRONIC WARFARE
- CYBER THREATS
- DIRECTED ENERGY
- SPACE SITUATIONAL AWARENESS
- POLICY, DOCTRINE, AND TRENDS



IMPORTANT NOTE

THIS PAGE LISTS THE PRIMARY SOURCE DOCUMENT USED AS THE FOUNDATION FOR THE SERIES. INDIVIDUAL INFOGRAPHICS MAY ALSO DRAW ON THE ANALYSIS CONTAINED WITHIN THIS REPORT.

COPYRIGHT AND LICENSING

COPYRIGHT AND LICENSE NOTICE

Copyright © 2026 NEWSPACEECONOMY.CA.

Except where otherwise noted, the original content of this document is licensed under the Creative Commons Attribution 4.0 International License. A copy of the license is available at <https://creativecommons.org/licenses/by/4.0/>.

NO ENDORSEMENT

References to organizations, products, services, technologies, publications, or individuals do not constitute or imply endorsement, recommendation, sponsorship, or approval by the author or publisher. Reuse of this document must not be represented as endorsed by the original author, publisher, or any person or organization identified for attribution.

ACCURACY AND COMPLETENESS

The information in this document is provided in good faith and was believed to be accurate at the time of publication. The author and publisher do not guarantee that the information is complete, current, error-free, or suitable for every purpose. Readers should independently verify information that may affect important decisions.

Feedback and Suggestions

This document is revised as its material is corrected and extended. Corrections, omissions, and suggestions for what a future edition should cover are all welcome, and are read by the people who maintain it. The most useful feedback names the page or the figure it is about, says what is wrong or missing, and — where it is a correction — points at a source. Feedback about the document as a whole, including whether it answered the question you opened it with, is just as welcome.

[Share your feedback on this document](#)

