APRIL 2025

A REPORT OF THE CSIS AEROSPACE SECURITY PROJECT

SPACE THREAT ASSESSMENT 2025

Authors
CLAYTON SWOPE
KARI A. BINGEN
MAKENA YOUNG
KENDRA LAFAVE

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

APRIL 2025

SPACE THREAT ASSESSMENT 2025

Authors
CLAYTON SWOPE
KARI A. BINGEN
MAKENA YOUNG
KENDRA LAFAVE

A REPORT OF THE
CSIS AEROSPACE SECURITY PROJECT

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

ABOUT CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

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

ABOUT ASP

The Aerospace Security Project (ASP) is a trusted resource for policymakers, offering insightful thoughts and in-depth analyses on policy issues, operational concepts, technology trends, and economic drivers in the space and air domains. Our mission is to educate and inform policymakers and the public, conduct independent research and analysis, and convene experts with broad perspectives to advance creative and practical solutions that address the security challenges facing the United States and our allies and partners. ASP also fosters the next generation of scholars in national security space and air power policy through fellowship and internship opportunities.

Part of the Defense and Security Department at CSIS, Aerospace Security is led by Senior Fellow Kari A. Bingen and includes a distinguished group of expert affiliates spanning national security, civilian, commercial, and international aerospace issues.

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

ACKNOWLEDGMENTS

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.

ASP would like to thank Dane Brumm, Jenny Christen, Hilary Cohen, Jim Cooper, Karen Cox, Hector Falcon, Benoit Figuet, Alyson Fredette-Graves, John Gass, Max Geissbuhler, Greg Gillinger, Bob Hall, Jason Lapadula, Mairead Levison, Kate Maliga, Darren McKnight, Erin Miller, Raphael Monstein, Nate Notargiacomo, Madeline Reto, Audrey Schaffer, Jade Stanton, Mallory Stewart, and Martin Strohmeier for contributing their time, energies, and resources to help produce this year's report. Thanks also to the operators of several private social media accounts for their prompt and thorough coverage of space safety events during the past year, including Jim Shell, COMSPOC, HEO, Integrity ISR, LeoLabs, LSAS Tec, s2a systems, and Slingshot Aerospace, which greatly benefited the report's authors.

Additionally, the authors would like to thank the CSIS publications team, Hunter Hallman, Phillip Meylan, Kelsey Hartman, and Madison Bruno, CSIS designers Sabina Huang and Lauren Bailey, and our external copyeditor, Katherine Stark. This annual report would not be possible without their thorough, responsive, and diligent work.

Special thanks also to ASP interns Ioannis Nikas, Anna Kelly, and Mia Thiagarajan for their work on the report, assisting with research and analysis of datasets. Finally, thanks to Victoria Samson and Laetitia Cesari for their partnership and willingness to continue collaboration with ASP on tracking and assessing global counterspace threats.

CONTENTS

INTRODUCTION

WELCOME TO THE *2025 SPACE THREAT ASSESSMENT* by the Aerospace Security Project at the Center for Strategic and International Studies (CSIS). This resource for policymakers and the public leverages open-source information to assess key developments in foreign counterspace weapons. Drawing on eight years of collected data and analyses, this series describes trends in the development, testing, and use of counterspace weapons and enables readers to develop a deeper understanding of threats to U.S. national security interests in space.

Since the publication of the 2024 *Space Threat Assessment*, there have been few headline-grabbing counterspace developments. No nation was known to have tested or used kinetic anti-satellite missiles, commonly called direct ascent anti-satellite (DA ASAT) weapons. There was no public indication that any nation tested or used counterspace weapons such as laser dazzlers or directed energy weapons. While Russia's pursuit of a nuclear anti-satellite capability topped the news last year, no information has publicly surfaced revealing how close Russia might be to launching this system, though the United States and its international partners remain concerned that Russia could decide to deploy such a weapon.[1]

But a closer look reveals that the past year, from the perspective of counterspace developments, has been anything but uneventful. Rather than entirely new developments, the past year mostly witnessed a continuation of the worrisome trends discussed in prior reports, notably widespread jamming and spoofing of GPS signals in and around conflict zones, including near and in Russia and throughout the Middle East.[2] Chinese and Russian satellites in both low Earth orbit (LEO) and geostationary Earth orbit (GEO) continue to display more and more advanced maneuvering capabilities, demonstrating operator proficiency and tactics, techniques, and procedures that can be used for space warfighting and alarming U.S. and allied officials.[3] Finally, U.S. companies providing a commercial space service to government users, particularly defense and military ones, remain squarely in the crosshairs of nation states, with Russia in particular vocal about its intention to consider commercial assets used by the U.S. military as legitimate targets.[4]

This past year also saw the growth of commercial and military dual-use technologies that could be modified to serve a counterspace purpose. Companies working on in-space servicing and debris removal reached important milestones, demonstrating their ability to conduct rendezvous, proximity, and docking operations, techniques that could be used by anti-satellite weapons. The behaviors of commercial satellites pursuing in-space servicing, inspection, debris removal, and other business use cases could easily be confused for counterspace operations, creating risks of misunderstandings and possibly unintended escalations in a crisis.

Though this report has not historically covered U.S. counterspace capabilities, it would be difficult to assess the global counterspace landscape without noting the evolving U.S. posture toward counterspace weapons and operations. In response to China's rapid buildup of military space capabilities in all orbital regimes, U.S. Space Force senior leaders have repeatedly emphasized over the last year that the United States is prepared to conduct offensive and defensive space operations and intends to field more counterspace capabilities.[5] This report also does not typically address unintentional debris creation in

orbit, but this year the assessment includes a discussion on the latent risks to space operations posed by accidental debris-causing events.

Finally, a common thread throughout this year's report is how space fits into the future of warfare. The normalization of space as a military operational domain and its integral role in joint operations mean that space is fair game during conflict. Warfighting will happen in, through, and from space, meaning that a future peer-on-peer conflict may very well bring disruption and destruction to space on the same scale that it would bring to other places closer to Earth. Counterspace threats should be viewed within the broader context of efforts by adversaries to degrade the ability of the United States and its allies to fight and win a war and disrupt the economy and day-to-day life on Earth, not merely as efforts to degrade a space capability. Overall, space is likely becoming a more dangerous place and woven ever more into both peacetime and wartime activities.

COUNTERSPACE WEAPONS

THIS CHAPTER PROVIDES AN OVERVIEW of different types of counterspace weapons and a useful taxonomy to classify and differentiate them. Counterspace weapons vary significantly in the technical methods they use to create effects against space systems, in how they are deployed, and in the level of technology and resources needed for their development and fielding. For the purposes of this report, counterspace weapons are organized into four main categories: kinetic, non-kinetic, and electronic weapons and cyber operations.

Kinetic weapons are defined here as those using physical, material means such as bombs, bullets, missiles, and other munitions. All kinetic weapons are considered as meant to destroy or damage. This category includes weapons that target spacecraft, such as DA ASAT missiles outfitted with conventional warheads, and projectile attacks launched from one on-orbit satellite to another. It also includes weapons that target terrestrial space infrastructure, such as ground stations, launch sites, rocket and satellite factories, and space monitoring infrastructure. Orbital grappling satellites are another form of kinetic weapon. Such a grappler physically handles a target spacecraft to do it harm or attaches itself to a spacecraft and maneuvers it to another location.

Non-kinetic weapons are defined as those that use radiated energy to destroy, damage, or interfere with space systems. This energy can be directed, such as with laser or microwave energy, or distributed through nuclear detonations or electromagnetic pulse (EMP) events. High-powered lasers and dazzlers and high-powered microwave ASAT systems are included in this category.

Illustration
A ballistic missile can be used as a kinetic counterspace weapon.

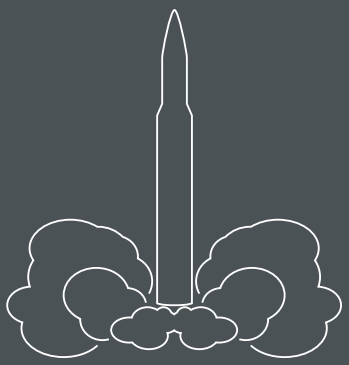


Table 1

COUNTERSPACE WEAPONS OF CHINA, RUSSIA, IRAN, AND NORTH KOREA AS OF MARCH 2025

	Kinetic Weapons			Non-Kinetic Weapons		Electronic Weapons		Cyber Operations
	Terrestrial Infrastructure Attack	Direct-Ascent ASAT	Orbital ASAT	Nuclear Detonation	Directed Energy	Jamming	Spoofing	
China	Yes	Yes	Maybe	Yes	Yes	Yes	Yes	Yes
Russia	Yes	Yes	Probably	Yes	Yes	Yes	Yes	Yes
Iran	Yes	No	No	No	No	Yes	Yes	Yes
North Korea	Yes	No	No	Yes	No	Yes	Yes	Yes

CSIS AEROSPACE SECURITY PROJECT RESEARCH AND ANALYSIS

Dazzlers are intended to temporarily blind an optical satellite, although they may also unintentionally damage targeted satellites. Nuclear detonations in the upper atmosphere or space are included in this category because these attacks primarily damage electronics through the resulting EMP and lingering radiation that gets trapped by Earth's magnetic field. Other nonnuclear weapons that create EMP events in space would also be included in this category.

Electronic weapons use the electromagnetic spectrum to deny or interfere with a target's ability to use space services and capabilities. These weapons cannot destroy; they only impart temporary effects for as long as the electronic system engages its target. This category includes jamming and spoofing of global navigation satellite system (GNSS) and satellite communications (SATCOM) signals. Spoofing, sometimes also called signal hijacking, is a form of electronic attack where an attacker tricks a receiver into believing a fake signal produced by the attacker is the real signal it is trying to receive. Also included in this category are any electronic attacks to jam space-based radar and the reception of radio frequency (RF) signals by the user of a satellite service on Earth, the satellite itself, or the ground station of a space system.

The final category, cyber operations, includes any offensive activity in cyberspace that targets space systems, including ground infrastructure, satellite terminals, spaceports, and spacecraft. Cyber operations can destroy or permanently disable a targeted system, although they can also be used to temporarily disrupt it or to conduct espionage, including gaining access to proprietary or sensitive technical information on a target network. A network exploitation can be a beachhead for any of these purposes, as a cyber operation's intent is often ambiguous.[1]

Many of these counterspace capabilities depend on robust space situational awareness (SSA) and intelligence information from both terrestrial and space-based platforms to target space systems and verify attack success.[2] In order to attack a satellite on-orbit, an aggressor would need to know its precise location and where it is moving. The aggressor will also want accurate battle damage assessments. For example, if a satellite is targeted through a cyberattack that allows the attacker to disable its controls, SSA or intelligence insights will be necessary to determine if the attack was successful by monitoring the satellite's movements and network activity. Although this report tracks counterspace weapons trends, it is important to acknowledge the critical data needed to develop and employ many of these weapons against their targets.

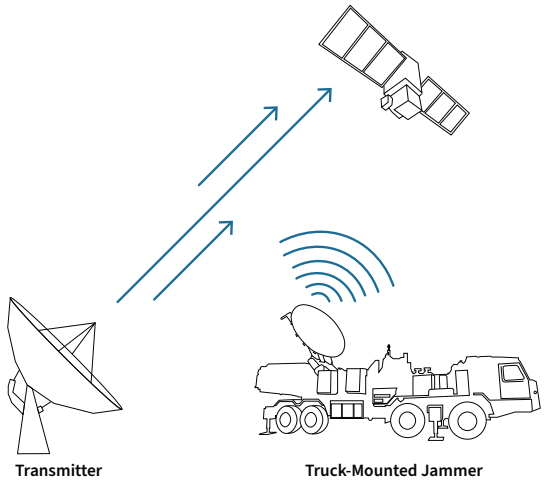


Illustration
Uplink jamming is a form of electronic counterspace attack.

Table 2

TYPES OF COUNTERSPACE WEAPONS

	Kinetic Weapons			Non-kinetic Weapons		Electronic Weapons		Cyber Operations
	Terrestrial Infrastructure Attack	Direct-Ascent ASAT	Orbital ASAT	Nuclear Detonations	Directed Energy	Jamming	Spoofing	
Origin to Destination	Ground-to-Ground	Ground-to-Space	Space-to-Space	Ground-to-Ground; Ground-to-Space; Space-to-Space	Ground-to-Ground; Ground-to-Space; Space-to-Space	Ground-to-Ground; Ground-to-Space; Space-to-Space	Ground-to-Ground; Ground-to-Space; Space-to-Space	N/A
Permanence of Attack	Permanent	Permanent	Permanent	Permanent	Varies, dependent on mode of attack	Not Permanent	Not Permanent	Varies, dependent on mode of attack
Scale of Attack Effects	Widespread, if node supports multiple satellites	Widespread, if orbital debris creation	Limited to Widespread, dependent on mode of attack	Widespread	Limited and Regional, dependent on mode of attack	Limited and Regional, dependent on mode of attack	Limited and Regional, dependent on mode of attack	Limited to Widespread, dependent on mode of attack
Attributability of Attack	Variable attribution, depending on mode of attack	Launch site can be attributed	Can be attributed by tracking previously known orbit	Launch site can be attributed	Limited attribution	Modest attribution depending on mode of attack	Modest attribution depending on mode of attack	Limited or uncertain attribution
Requires Space Launch Capability	No	Yes	Yes	No	No	No	No	No
Requires Space Domain Awareness	No	Yes	Yes	No	Yes	No	No	No

CSIS AEROSPACE SECURITY PROJECT RESEARCH AND ANALYSIS

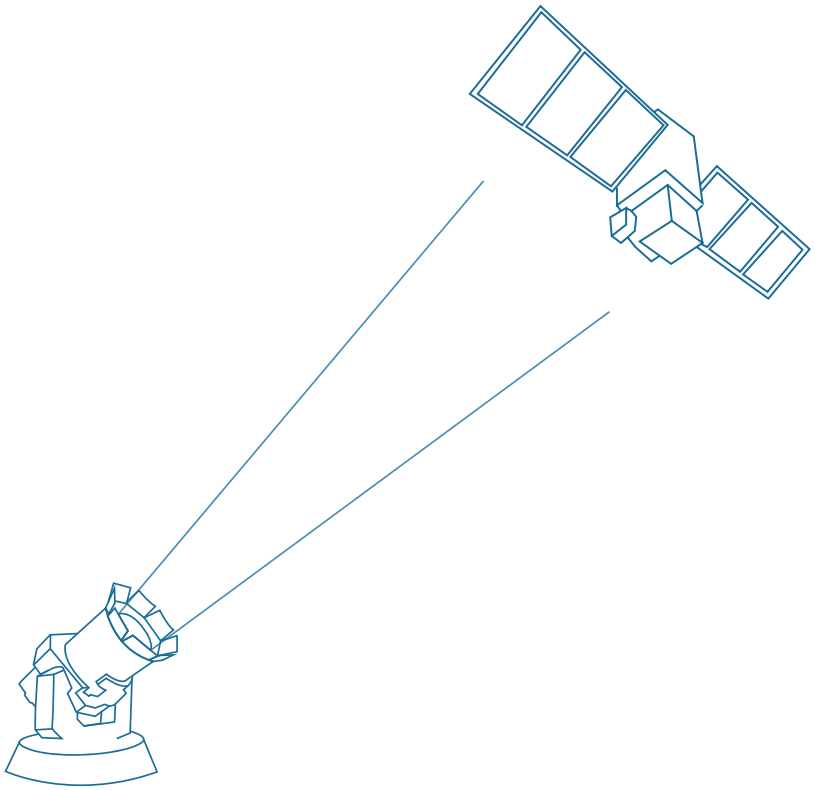


Illustration A laser is an example of a non-kinetic counterspace weapon.

CHINA

BEIJING'S ACTIONS OVER THE LAST YEAR point to an ever-increasing emphasis by the People's Republic of China (PRC) on the military use of space. Since the publication of the last threat report, continuing past trends, China demonstrated dual-use, highly maneuverable satellites in orbit and the tendency to maneuver and use fuel seemingly without regret. These activities point to growing operator proficiency and maturing space tactics, techniques, and procedures. Beijing also reorganized its armed forces, creating a specific force oriented around space operations. Though China has continued its aggressive cyber operations, few seem to specifically target space systems. Additionally, PRC officials and academics are more willing to publicly criticize U.S. behaviors in space, pointing to examples of where they claim the United States engages in the same space activities for which it criticizes China.[1]

Over the last year, the most concerning development to U.S. observers should be the launch and operation of increasingly advanced Chinese satellites. China continues to launch and operate highly maneuverable satellites, demonstrating an advanced level of technological and operational acumen that, if not already deployed for such purposes, could enable a formidable on-orbit counterspace arsenal. Through the use of these satellites, Chinese operators are gaining experience in developing tactics and procedures that can be used for space warfighting, to include both defensive and offensive advanced space operations. Additionally, China is dramatically increasing its space launch capability, with several commercial providers coming online in the next few years.[2] Each year, the PRC is launching more and more satellites, making characterization of those satellites more challenging year after year.[3]

Continuing trends described in prior editions of *Space Threat Assessment*, U.S. experts and military officials expressed concerns in December 2024 about unusual and potentially threatening behaviors of Chinese satellites in GEO.[4] According to an expert at ExoAnalytic, these behaviors demonstrate China's proficiency in conducting sophisticated satellite maneuvering and willingness to expend fuel to conduct rapid maneuvers.[5] To emphasize these points, the expert also noted that the Chinese satellite TJS-2 was tracked during the last year maneuvering at 44 meters per second, which is unusually high and uses significantly more fuel than the more standard range of 0.5–1 meters per second for repositioning satellites in GEO.[6] The expert further described how another satellite, TJS-4, maneuvered to position itself between a U.S. space surveillance satellite and the Sun, creating a disadvantageous geometry for imaging the Chinese satellite.

The following three Chinese satellite programs usually feature prominently in each edition of *Space Threat Assessment*, and this year is no exception. There is often little public information about these spacecraft capabilities or specific missions, outside of official Chinese government statements, which are almost certainly designed to conceal the true purposes of military satellites. Most public information about the activities of Chinese satellites in GEO, documenting the sophistication and frequency of Chinese satellite maneuvers, was provided by SSA companies sharing their observations on social media platforms. Integrity ISR, a space and intelligence, surveillance, and reconnaissance (ISR) training company, and LSAS Tec, a company providing support services for space operations, released a video on YouTube documenting several TJS-10 maneuvers in May 2024 that eventually brought the satellite to within 25 kilometers (km) of another Chinese satellite in GEO, TJS-3, on May 16, 2024.[7]

CHINA CONTINUES TO LAUNCH AND OPERATE HIGHLY MANEUVERABLE SATELLITES, [WHICH] COULD ENABLE A FORMIDABLE ON-ORBIT COUNTERSPACE ARSENAL.

In January 2025, China launched SJ-25, which official sources claim will be used for testing satellite fuel replenishment and life extension service technologies.[8] After launch, according to analysis from COMSPOC and Integrity ISR, SJ-25 entered a coplanar orbit with SJ-21, a satellite which in 2022 attached to and moved a defunct Beidou satellite from its position in GEO to a graveyard orbit, suggesting SJ-25 may intend to refuel SJ-21.[9] Additionally, in January 2025, suspected Chinese GEO inspector satellite TJS-3 moved to within one degree latitude of SJ-21, possibly suggesting a supporting role for TJS-3 in an upcoming refueling attempt.[10]

On two occasions in the last year, Integrity ISR published an analysis on the behaviors of SY-12-01 and SY-12-02, a pair of satellites launched in December 2021 whose purpose

Table 3

CHINESE SATELLITE SERIES THAT OFTEN EXHIBIT RPOS

Program	English Translation[11]	Satellites Entered into Operation*	Orbit	Purpose
Tongxin Jishu Shiyan (TJS)	"communication technology test"	17	GEO	suspected military early warning and signals intelligence missions
Shijian (SJ)	"best practice" or "put into practice"	43	LEO, GEO, Sun-Synchronous Orbit (SSO), and Highly Elliptical Orbit (HEO)	various experimental missions
Shiyan (SY)	"experiment," "pilot," or "trial"	45	LEO, GEO, SSO, and HEO	various experimental missions

***INCLUDES OPERATIONAL, DECAYED, AND FAILED MISSIONS**
CSIS AEROSPACE SECURITY PROJECT RESEARCH AND ANALYSIS, CURRENT AS OF APRIL 18, 2025

is described by Chinese media as "spatial environment exploration and related technical tests."[12] At the time of publication for last year's *Space Threat Assessment*, these satellites had been drifting in opposite directions across the entire GEO belt. They continued to drift this year. According to the Integrity ISR assessments, in November 2024, SY-12-02 reached its turnaround point of 17.3 degrees east (over central Europe) and began a new eastward journey.[13] In September 2024, SY-12-01 reached its turnaround point of 178.9 degrees east (over the Pacific Ocean) and began a new westward journey.[14]

In addition to its progress in GEO, over the last year China has demonstrated the ability to execute increasingly complicated spacecraft maneuvering in LEO. In May 2024, the Shenlong space plane released, maneuvered with, and possibly captured an object before returning to Earth in September 2024, after having been in orbit for over 260 days, according to analysis by Slingshot Aerospace.[15] The space plane had previously released six other space objects soon after it launched in December 2023.[16] In January 2024, three satellites believed to be technology demonstrators—SY-24C-01, SY-24C-02, and SY-24C-03—conducted corkscrew maneuvers around SJ-6-05B, believed to be another technology demonstrator with potential signals collection capability, as described in an analysis by Integrity ISR.[17] Additionally, in March and April 2024, SY-24C-03 and SJ-6-05A conducted rendezvous and proximity operations (RPO), with each satellite maneuvering and the closest approach distance less than 1 km—essentially face-to-face for satellites traveling at around 17,000 mph—on April 22, 2024, according to analysis by s2a solutions, a Swiss company.[18] In March 2025, a senior Space Force official characterized these behaviors as "dogfighting" in space.[19]

While continuing to advance its abilities to conduct sophisticated maneuvering in both LEO and GEO, according to a study released by the China Aerospace Studies Institute (CASI) in September 2024, China is also monitoring and assessing U.S. space-based SSA capabilities and is more willing to publicize the results of its assessments.[20] The CASI report details the increasing number of Chinese academic publications that analyze the patterns of life of U.S. Geosynchronous Space Situational Awareness Program (GSSAP) satellites, including publicly naming the satellites most visited by GSSAP. China likely obtains data on close approaches from its own sensors, the Russian-led International Scientific Optical Network (ISON), and publicly available information from U.S. and European SSA databases.[21] The PRC's SSA capabilities rely on domestic ground-based infrastructure, foreign datasets, and at least 10 spacecraft.[22]

Test satellite Shijian-25 is sent into space on January 7, 2025.

PHOTO BY DU XINXIN/GETTY IMAGES

From an operational standpoint, China's attention to the patterns of life of U.S. spacecraft has likely influenced how Chinese satellites respond when approached by suspected U.S. space surveillance satellites. Notable examples of such behavior in GEO include how SY-12-01 and SY-12-02 responded to the approach of USA 270 in late 2023 and TJS-4 behaviors described by ExoAnalytic and noted earlier in this section. Integrity ISR and LSAS Tec published information about maneuvers over several months in late 2024 by LDPE-3A, a U.S. satellite characterized as a "freight train" for experiments to GEO, that placed it about 25 km from and with favorable lighting conditions for viewing Chinese satellite SJ-23, which in this case did not maneuver in response.[23] China is likely increasingly willing to publicly discuss observed GSSAP behaviors to influence international opinions, probably aiming to portray the United States as having a double standard—engaging in the same activities for which it criticizes China as being unsafe and unprofessional.

There is little public information on new Chinese cyber or electronic warfare activities since the last *Space Threat Assessment*. During the last year, experts expressed concerns about the impacts of Chinese-attributed Salt Typhoon cyber operations on space infrastructure.[24] More detailed information was officially released on another PRC state-sponsored cyber group targeting satellite services and other sectors, Volt Typhoon, including descriptions of the actor's techniques and recommended remedies.[25] Additionally, public threat reporting from September 2024 indicated that an unknown cyber threat actor tied to Chinese-speaking groups has focused on supply chains for defense-related industries, with a particular focus on drone manufacturers, in Taiwan.[26] It would be reasonable to assume these Chinese-speaking groups were affiliated in

some way with China. It has been mostly quiet on the electronic warfare front, as there were only sporadic reports of Chinese jamming or spoofing of GPS or other satellite signals over the last year.[27] Though there is not much cyber or jamming news this past year, based on findings presented in prior editions of *Space Threat Assessment*, China undoubtedly maintains advanced cyber and electronic warfare capabilities that can affect space systems.[28]

A reorganization of China's armed forces during the last year points to a focus on warfighting in space, as well as in cyberspace and the information operations domain, that cuts across and supports the service branches. Specifically, in April 2024, China announced the reorganization of the People's Liberation Army (PLA) into four services—the PLA Ground Force, Navy, Air Force, and Rocket Force—and four cross-cutting arms—the PLA Aerospace Force, Cyberspace Force, Information Support Force, and Joint Logistics Support Force.[29] Though the Joint Logistics Support Force has existed since 2016, the Aerospace Force, Cyberspace Force, and Information Support Force are new organizations, created by dividing up the responsibilities of the now defunct Strategic Support Force, which had previously handled space-based intelligence, reconnaissance, electronic countermeasures, signals intelligence, information warfare, and communications. The Aerospace Force is responsible for managing all PLA space-based capabilities, including counterspace weapons, and PLA space launch facilities.

Throughout the last year, Chinese scientists published several research papers on military technologies, including high-powered microwave and laser technologies, that—though not described as counterspace weapons in the papers—could be applied to counterspace weapons developments.[30] However, there is no new publicly available information on specific military programs aimed at developing or testing these technologies. As noted in *Space Threat Assessment* 2024, the PRC has already fielded ground-based laser weapons capable of blinding or damaging satellites and conducted research on mobile high-powered microwave weapons for general military applications.[31] China also maintains the same wide range of both fixed and mobile electronic warfare systems that can interfere with satellite communications links, GNSS signals, and synthetic aperture radar (SAR) intelligence-gathering satellites, as described in the 2024 report.

CHINA IS LIKELY INCREASINGLY WILLING TO PUBLICLY DISCUSS OBSERVED GSSAP BEHAVIORS TO INFLUENCE INTERNATIONAL OPINIONS.

Over the past year, it has also become clear that Beijing assesses a military threat posed by LEO systems like Starlink. Researchers at East China Normal University and the PLA-affiliated National University of Defense Technology have written about the military and strategic implications of Starlink satellites, arguing that SpaceX's relationship with the U.S. government may have lasting security implications. Three articles, published in Chinese journals focused on intelligence and international security studies, outline concerns of broad deployment of Starlink satellites by the United States and Starlink's ability to transmit data that may be used for new combat styles, citing the impact Starlink had on the battlefield in Ukraine.[32] Importantly, these assessments overstate the capabilities of Starlink and assume the satellites have been integrated into U.S. Department of Defense (DOD) architectures and intelligence missions. Further, as one U.S. scholar observes, a "clear PRC concern that emerges from these articles is that China's counterspace capabilities will be less effective against a U.S. satellite constellation composed of a mix of proliferated constellations."[33]

In early 2025 it was reported that Chinese scientists have run artificial intelligence-created simulations of targeted attacks on Starlink satellites to disrupt services.[34] A Nanjing University of Aeronautics and Astronautics team published a study that alleges 99 Chinese satellites could disrupt 1,400 Starlink satellites within a 12-hour period, targeting not individual satellites, but large sections of the Starlink constellation.[35] Inspired by how whales hunt in teams and direct large swaths of fish into their mouths in open water, the study describes Chinese satellites "hunting" Starlink satellites by using directed-energy weapons, such as lasers and microwaves. Notably, Nanjing University has been called one of the "seven sons" of China's national defense, founded by the Chinese Ministry of National Defense and sanctioned by the United States and Taiwan for its involvement in developing military technologies.[36]

RUSSIA

THROUGHOUT THE PAST YEAR, Russia has engaged in several provocative counterspace activities, in addition to allegedly working on a nuclear space-based anti-satellite weapon, according to revelations that first surfaced in February 2024.[1] In May 2024, the United States accused Russia of launching a counterspace weapon, assessing it had "characteristics resembling previously deployed counterspace payloads" in 2019 and 2022.[2] Not long after launch, the Russian satellite, designated Cosmos 2576, proceeded to enter into a coplanar orbit with a U.S. government satellite, USA 314, maneuvers the U.S. government justifiably viewed with concern, as such actions could signal the positioning of a counterspace weapon.[3]

As of late February 2025, Cosmos 2576 was no longer operating in a synchronized orbit with USA 314, having begun maneuvers to raise its orbit in mid-February 2025, possibly coinciding with the thaw in U.S.-Russian relations.[4] In February 2025, Russia launched Cosmos 2581, Cosmos 2582, and Cosmos 2583, acknowledged by Moscow as belonging to the Ministry of Defense, but little else is publicly known about their mission.[5] Since then, Cosmos 2581 and Cosmos 2582 have moved in formation, coming as close as 100 meters apart on March 5, 2025—by any measure, a very close approach for two satellites.[6] Though Cosmos 2583 has yet to maneuver since reaching orbit, it did pass as close as 0.5 km to Cosmos 2581 and Cosmos 2582 on March 7, 2025.[7] Additionally, as it has done since its launch in August 2022, Cosmos 2558—a satellite that the U.S. Space Force asserts is also a counterspace weapon—remained in a coplanar orbit with USA 326.[8]

Meanwhile, Russia's Luch (Olymp) satellites have continued to prowl the GEO belt. Since the publication of the last *Space Threat Assessment*, Luch (Olymp) 2 has spent time near Eutelsat Konnect, RASCOM-QAF 1, Astra 4A (originally Sirius 4), Thor 7, SES 5, Intelsat 3-F7, Thor 6, and Intelsat 10-02, according to data from Slingshot Aerospace.[9] These satellites provide communications and broadcast services to a wide range of areas, including Africa, Europe, the Middle East, and South America. Some analysts assess that Luch (Olymp) 2 may have come as close as 5 km to Thor 7 in July 2024 and less than 1 km from Intelsat 10-02 in January 2025.[10] Believed to be a signals collection satellite, it is not surprising that Luch (Olymp) 2 loitered near satellites providing data and broadcast services over Europe, consistent with past Luch behavior.[11] Prior to the arrival of Luch (Olymp) 2 near Astra 4A in March 2024 (providing internet services across Europe), Astra 4A signals were jammed—likely by ground-based Russian jammers—interfering with Ukrainian broadcasts.[12] Though unlikely mere coincidence, the specific relationship between the two events is not clear. Since 2023, Luch (Olymp) 1 had been parked near Intelsat 37e at 342 degrees East latitude, though in March 2025 it moved slightly lower than the geostationary belt, starting an eastward drift of about half a degree per day.[13]

Though revelations that Moscow is developing a space-based nuclear anti-satellite weapon were covered in last year's assessment, this issue continued to develop throughout last year and remained a significant counterspace headline in 2024. Not long after the first reports surfaced in February 2024, U.S. officials publicly addressed their concerns that Russia was developing a "troubling" anti-satellite counterspace weapon with alleged nuclear capabilities.[14] A breach of the 1967 Outer Space Treaty (OST), which prohibits signatory nations from stationing nuclear weapons in space, such a weapon would disable or destroy hundreds—if not thousands—of satellites in LEO through radiation effects or the resulting EMP.[15] The United States not only publicly condemned the development of this new weapon but also sought to apply international pressure through the United Nations. To date, Russian officials continue to deny accusations that Russia is even pursuing such a weapon.

AS OF LATE FEBRUARY 2025, COSMOS 2576 WAS NO LONGER OPERATING IN A SYNCHRONIZED ORBIT WITH USA 314.

On March 14, 2024, the United States and Japan introduced a draft resolution to reaffirm states' obligations under Article IV of the OST, calling on nations not to develop nuclear weapons specifically designed to be placed in orbit around the Earth. The draft resolution underwent a series of negotiations and redrafts leading to a vote on April 24, 2024. While 65 member states cosponsored the draft resolution, Russia cast a veto, and the draft resolution failed to be adopted. China abstained from the vote. The United States and Japan released a joint statement expressing their disappointment and continued commitment to ensuring countries cannot deploy nuclear weapons in space. Soon after, Russia and China circulated their own resolution calling on broad international prohibitions on space weapons. As it has done when Russia and China raised such language in the past, the United States opposed this resolution, previously calling the Russian and Chinese proposal fundamentally flawed and noting that it lacks a verification mechanism and does not address ground-based ASAT weapons.[16]

Piecing together statements from U.S. officials and other publicly available sources, it appears that Russia has not yet launched an anti-satellite weapon with a nuclear payload. However, it was disclosed that Moscow's efforts have been years in the making, with a senior U.S. official shedding light on the intended orbital regime for such a counterspace weapon and connecting a "scientific" satellite currently in-orbit "in a region not used by any other spacecraft . . . of higher radiation than normal lower-Earth orbits" to the effort.[17] Satellite trackers deduced that the satellite is likely Cosmos-2553, a satellite launched in February 2022 into a 2,000 km orbit that the Russian ministry of defense stated was a "technological spacecraft . . . equipped with newly developed onboard instruments and systems for testing them under the influence of radiation and heavy charged particles."[18]

While reports claim this satellite carries a "dummy warhead," U.S. officials stress that, should a nuclear weapon be detonated at a 2,000 km altitude, the effects would be "indiscriminate" and render LEO unusable "for some period of time," perhaps a year.[19] The only other satellites in orbits near Cosmos-2553 are one nonoperational Russian satellite and 10 nonoperational U.S. satellites. According to one expert, if the satellite is testing new technologies, it may have been placed in such a remote orbit because there would be less risk of affecting other satellites and it would be difficult to monitor.[20] Based upon persistent radar monitoring by LeoLabs of Cosmos-2553, there is high confidence it has been tumbling since mid-November 2024.[21] This observation strongly suggests the satellite is no longer operational.

In addition to its counterspace efforts in space, Russia engages in jamming and spoofing GPS signals on Earth. Russian efforts to interfere with GPS signals stretch from the Baltic and Nordic nations, through Ukraine and Russia itself, to countries in the Black Sea region.[22] Though efforts to jam and spoof GPS in Ukraine, including around Crimea in the Black Sea, have been ongoing since the start of the war, those efforts mushroomed to include many other regions in mid-2024.[23]

Figure 1

TIMELINE OF RUSSIAN NUCLEAR ASAT THREAT AND RESULTING DEVELOPMENTS

FEBRUARY 14, 2024

U.S. House Permanent Select Committee on Intelligence Chairman Michael Turner issues a cryptic statement “concerning a serious national security threat” that press reports later reveal as a potential Russian nuclear anti-satellite weapon designed to target satellites orbiting the Earth.

FEBRUARY 15, 2024

During a press conference, a White House spokesperson, John Kirby, confirmed that Russia has obtained a "troubling" new ASAT weapon, an accusation that Russia denied as a "malicious fabrication.”

FEBRUARY 20, 2024

Russian President Vladimir Putin comments on the topic of nuclear weapons in space during a working meeting in Moscow with Russian Defense Minister Sergei Shoigu, “Our position is clear and transparent: We have always been categorially against, and are now against, the placement of nuclear weapons in space. . . . On the contrary, we call for compliance with all agreements that exist in this area and proposed to strengthen this joint work many times over.”

MARCH 14, 2024

The United States and Japan circulate a draft resolution to the UN Security Council that would affirm the goal of preventing an arms race in space and reiterate the Outer Space Treaty’s prohibition on placement in Earth orbit of objects carrying nuclear weapons or any other kinds of weapon of mass destruction.

APRIL 24, 2024

The UN Security Council votes—13 votes in favor, 1 against (Russia), and 1 abstention (China)—on the draft resolution which fails to be adopted due to Russia's veto. Russia and China had proposed an amendment to the draft resolution calling for a ban on placing any weapons in space. The amendment was not adopted because it failed to get the minimum level of support in the UN Security Council needed to add an amendment.

MAY 1, 2024

U.S. Assistant Secretary of Defense for Space Policy John Plumb testifies before the U.S. House Armed Services Committee that Russia is developing a nuclear ASAT weapon intended to "fly in space" that, while "not an imminent threat," could render LEO unusable "for some period of time," perhaps a year, if detonated.

MAY 3, 2024

U.S. Assistant Secretary of State for Arms Control, Deterrence, and Stability Mallory Stewart discusses concerns that Moscow is "considering the incorporation of nuclear weapons into its counterspace programs." She further says that the United States had been aware of this effort for years and gave clues about the intended orbital regime and a connected "scientific" satellite currently in-orbit "in a region not used by any other spacecraft . . . of higher radiation than normal lower-Earth orbits."

MAY 20, 2024

The UN Security Council votes on a Russian-led draft resolution, containing similar language as the U.S.-Japan–led resolution vetoed by Russia on April 24, 2024, with the addition of the previous Russia-China–led amendment and text calling for negotiations on a legally binding agreement for the prevention of an arms race in outer space. The UN Security Council does not adopt the resolution—seven votes in favor, seven votes against, and one abstention (Switzerland).

JUNE 20, 2024

Chairman Turner deliveres remarks at CSIS warning of the threat posed by a Russian nuclear ASAT weapon.

MARCH 26, 2025

In his written testimony to the House Armed Services Committee, Subcommittee on Strategic Forces, the Commander of U.S. Space Command General Stephen N. Whiting describes Russia's placement of a nuclear weapon in space as "most concerning," noting its ability to potentially disrupt the use of space.

THE HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE, THE WHITE HOUSE, BBC NEWS, THE HOUSE ARMED SERVICES COMMITTEE, CSIS, AND THE SENATE ARMED SERVICES COMMITTEE

RUSSIAN EFFORTS TO INTERFERE WITH GPS SIGNALS STRETCH FROM THE BALTIC AND NORDIC NATIONS . . . TO COUNTRIES IN THE BLACK SEA REGION.

GPS interference in the Nordic and Baltic regions is not new. For example, in the fall of 2018, Norway accused the Russian military of jamming GPS signals in the Kola Peninsula during NATO's largest military exercise since the Cold War.[24] However, the past two years have seen a surge in reports of GPS interference in these regions, as noted by the Finnish transport and communications agency Traficom, which saw roughly 2,000 reports filed in 2024 compared to 239 reports in 2023.[25] While it is difficult to point to a clear explanation for Russia's interest in jamming and spoofing GPS signals across these regions, the growth of GPS interference in Russia itself is a response to Ukrainian attacks on Russia using GPS-guided drones and missiles as point defense.[26]

Russia has also tried to interfere with Ukrainian television broadcasts from satellites, including attempting to jam signals from one of the Amos satellites in August 2024.[27] Additionally, television signal jamming and hijacking affected Ukrainian broadcasts on Eutelsat's Hotbird in March and April 2024.[28] In response to increased jamming over the last year, a number of European countries lodged complaints with the International Telecommunication Union in June 2024, which then condemned Russian interference with GPS and television signals.[29]

Russia has on at least one occasion during the last year employed electronic warfare activities outside of Ukraine that affected more than GPS and television signals. In March 2024, when flying near Kaliningrad, a UK military aircraft returning a senior official to the United Kingdom from a visit to Poland experienced GPS and communications interference for about 30 minutes.[30] It remains unclear whether the official's flight was the specific target of the jamming attack, with UK officials publicly noting that it is not uncommon for aircraft to experience GPS interference near Kaliningrad. Russia also continues to pursue capabilities designed to defeat Starlink, having announced in December 2024 the development of a new monitoring system called Kalinka that can identify and locate Starlink terminals.[31]

As it has done in prior years, Russia threatened the private sector for supporting the U.S. national security mission in space. In March 2024, a spokesperson for Russia's Ministry of Foreign Affairs said that Russia is "aware of Washington's efforts to attract the private sector to serve its military space ambitions," and that such systems "become a legitimate target for retaliatory measures, including military ones."[32] Russia also complained during the UN General Assembly in October 2024 that the United States and its allies use civilian and commercial space infrastructure for military purposes, arguing that such activities jeopardize the peaceful use of space.[33]

OTHERS

IRAN

Since the beginning of last year, Iran has continued to increase its proficiency in space launch, successfully launching satellites in January 2024, September 2024, and December 2024 from Iranian launch sites.[1] The December 2024 launch placed three satellites into orbit. Iran claimed one of those three satellites was a space tug, called Saman-1, that could reposition other satellites in orbit, a capability with obvious counterspace uses.[2] In November 2024, Russia launched two Iranian remote sensing satellites, called Kowsar and Hodhod, which Iran claims are the first two satellites operated by its private sector.[3] Russia has launched other Iranian satellites before, including Iran's first satellite, Khayyam, in August 2022.[4]

Iran has pursued cyberattacks against aerospace and satellite infrastructure, among other targets, over the last year.[5] Microsoft and Palo Alto Networks published reports in March and August 2024, respectively, that provided more details on the Peach Sandstorm incidents.[6] Both reports assessed that this cyber campaign was directed by the Iranian Islamic Revolutionary Guard Corps as part of ongoing efforts to gather intelligence and conduct social engineering attacks. According to Microsoft, this same Iranian cyber threat actor has conducted prior attacks targeting the aerospace, construction, defense, education, energy, financial services, healthcare, government, satellite, and communications sectors in multiple countries.[7] In February 2024, Mandiant reported on malicious cyber activity, aimed at espionage, linked to Iran's Islamic Revolutionary Guard Corps that targeted the aerospace and defense sectors in the Middle East and possibly Turkey, India, and Albania.[8]

NORTH KOREA

North Korea's only space launch attempt in 2024 ended in failure when a rocket carrying the country's second reconnaissance satellite exploded after liftoff in May 2024.[9] North Korea continues to operate its Mallygyong-1 satellite, which was launched in November 2023, and executed maneuvers to raise the satellite's altitude in February and June 2024.[10] It was reported that North Korea successfully tested a new ballistic missile in October 2024 and new intermediate-range hypersonic missile in January 2025, which followed a prior test in April 2024.[11] Though none of these developments specifically relate to counterspace weapons, they demonstrate increasing North Korean proficiency with space, missile, and rocket technologies.

During the past year, South Korea repeatedly raised concerns about North Korean efforts to jam GPS signals around the Korean Peninsula and near the border between North and South Korea. Without providing more specific information, in January 2025, then–U.S. Secretary of State Antony Blinken warned that Russia was close to sharing "advanced space and satellite technology" with North Korea.[12]

In July 2024, the FBI and other partners issued a joint cybersecurity advisory warning of North Korean cyber espionage activities targeting defense, aerospace, nuclear, and engineering entities around the globe with the goal of advancing North Korea's military and nuclear capabilities.[13] Mandiant identified a cyber threat group in June 2024 with probable ties to North Korea that conducted phishing attacks pretending to be from an energy company and aerospace industry entity while targeting other entities in those sectors.[14]

INDIA

In January 2025, the Indian Space Research Organisation's Space Docking Experiment (SpaDeX) mission successfully demonstrated India's ability to conduct rendezvous and proximity operations and docking activities.[15] Though not publicly associated with a military program, such capabilities have clear counterspace uses. As of December 2024, India may be in talks with Russia to acquire a ballistic missile early warning and space surveillance radar with a 6,000-km range for placement in southern India.[16] Such a system may be intended for monitoring missile launches from Pakistan, though it could also play a role in monitoring satellites and space objects.

South Korean news broadcast shows North Korea's launch of its Malligyong-1 satellite in November 2023.

JUNG YEON-JE/GETTY IMAGES

ISRAEL

Though Israel has not featured prominently in past editions of *Space Threat Assessment*, it is hard to ignore this year due to its efforts to interfere with GPS in the eastern part of the Mediterranean Sea, Syria, Lebanon, parts of Egypt, and Israel itself. No doubt aiming to protect itself from missile and drone threats launched by Iran, Hamas, Hezbollah, and the Houthis, Israel conducted markedly more widespread, persistent GPS jamming and spoofing, specifically around April 2024, when it was expecting Iranian retaliation to an Israeli strike in Syria that killed two senior Iranian officials.[17]

Israel continues to develop and refine directed-energy weapons, such as Iron Beam, for use in missile defense. While it does not appear that Israel intends to use these weapons for a counterspace purpose, Israel effectively maintains a latent anti-satellite capability, particularly when paired with its satellite detection and tracking knowledge. Israel likely conducted an exoatmospheric missile intercept in November 2024 when it shot down a Houthi ballistic missile.

EUROPE

Only two countries in Europe made counterspace news over the last year—France and Germany—with both countries publicly describing new counterspace initiatives. These would involve deploying satellites capable of performing inspection and space domain awareness (SDA) missions, as well as roles protecting other satellites from attack, possibly using lasers or other non-kinetic weapons. The new French program, called Toutatis, would include two LEO satellites: Lisa-1, performing an SDA mission, and Splinter LEO, a highly maneuverable satellite capable of tracking hostile satellites and potentially positioning itself between a hostile satellite and the target satellite.[18] Germany plans to launch the German Inspector Satellite for Multiple Operations.[19] The satellite, publicly revealed in 2024, would be equipped with robotic arms and be capable of inspecting other satellites.

FEATURED ANALYSIS

GPS JAMMING AND SPOOFING

LAST YEAR'S *SPACE THREAT ASSESSMENT* NOTED that GPS jamming and spoofing were becoming ubiquitous across parts of the world, particularly in areas of active military conflict. This past year saw a continuation and growth of that same trend. Many regions of the world, from the Arctic through Eastern Europe, to the Middle East and parts of South Asia, have been affected by GPS jamming and spoofing nearly every day since the publication of last year's report.

Though difficult to measure, the societal and economic impacts of such long-term disruptions to GPS service are significant, and no doubt compounded by ongoing conflict and political strife affecting many of these same areas. Qualitatively, however, GPS interference disrupts the lives and work of millions of people and in some cases (such as civil and commercial aviation) poses significant risks to public safety. Several UN agencies have also emphasized the harms of jamming and spoofing, noting that interference with satellite navigation signals is a threat to air and maritime safety and security.[1]

But GPS jamming and spoofing have produced—at least in part—the desired military effect, as munitions and drones that rely on GPS to find their targets have been made significantly less effective in GPS-denied environments.[2] That said, there is no sign that GPS interference is an air defense magic bullet. It is the many layers of modern integrated air defense systems, including jamming and spoofing, that have demonstrated effectiveness at blunting, for example, air threats to Israel and Russian drone and missile attacks on Ukraine. Likewise, the United States and European countries are implementing technical measures and operational techniques to mitigate such effects on their weapon systems.[3] Employing such GNSS jamming and spoofing systems to protect military and other critical infrastructure from attack—whether in Israel, Ukraine, or Russia—demonstrates the increasing tactical battlefield utility of counterspace weapons, and it is a trend that is expected to continue.

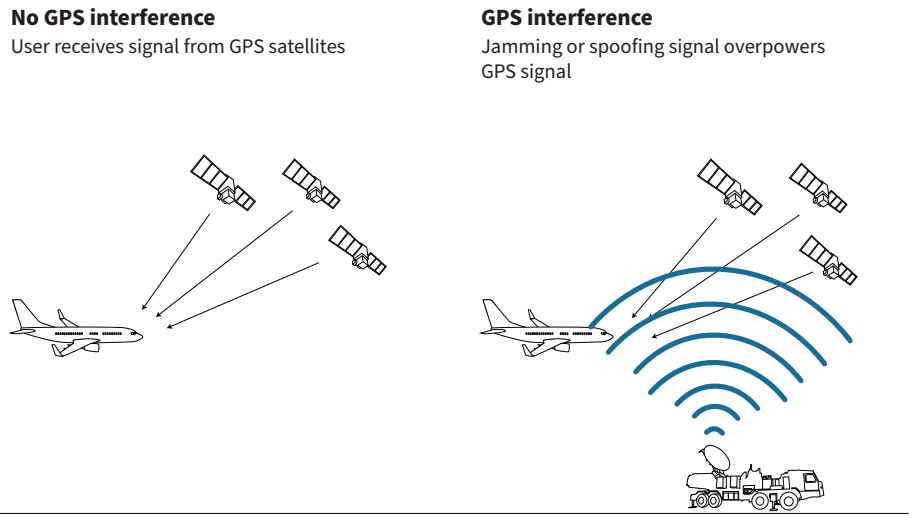
The most complete public picture of GPS interference around the globe at any point in time comes from maritime automatic identification system (AIS) and Automatic Dependent Surveillance-Broadcast (ADS-B) aircraft transponder signals. Aircraft pilots and drone operators have also been able to report instances of GPS jamming and spoofing through the Federal Aviation Administration's (FAA) Aviation Safety Reporting System and through a dedicated portal for reporting GPS anomalies.[4]

The International Air Transport Association also operates databases containing information about instances of GPS interference: the Incident Data eXchange, a tool for reporting flight security and safety concerns, and the Flight Data eXchange, a global flight data repository. NOTAMs (originally called Notices to Airmen), issued by national aviation authorities to warn pilots about possible GPS interference, can also provide clues about the location and timing of GPS anomalies.

Until the last five years, though not entirely uncommon, GPS jamming did not have a widespread or persistent impact on global aviation. Although other instances undoubtedly went unreported, between 2013 and 2017, only 90 reports of GPS jamming worldwide were logged in the Aviation Safety Reporting System. On the whole, these reports describe localized, ephemeral events.[5] For example, in 2015, one of these incidents involved intermittent GPS interference near a regional airport in Philadelphia that Federal Communications Commission agents attributed to a jammer being used by a driver to disable the tracking feature on his truck.[6] Several other reports in 2014 and 2015 related to GPS disruptions near a Mexico City airport that could have been caused by jamming.[7]

Figure 2

NORMAL GPS RECEPTION VS GPS JAMMING AND SPOOFING



GPS SPOOFING WORKGROUP, ***GPS SPOOFING***

Until 2017, when several ships reported GPS spoofing in the Black Sea, documented incidents of spoofing were still rare and mostly corresponded to transient events, such as the protection of traveling high-level government officials in Russia.[8] As recently as the start of Russia's invasion of Ukraine in February 2022, widespread reports of GPS spoofing were mainly confined to the Middle East.[9] But Ukrainian drone attacks into Russia provoked an increase in spoofing by Russian forces not just in Ukraine, but also across western Russia. Russian spoofing of GPS in the Baltic Region is harder to explain as a Russian force-protection measure due to its distance from Ukraine. It is instead likely an example of Russian use of hybrid warfare directed at NATO's newest members, as the rise in spoofing responds to the timing of their ascension to the alliance in spring of 2024.[10]

Today, Russian efforts to spoof GPS signals extend from the Black Sea to the Arctic, with impacts to several NATO members, and include many major cities and regions in Russia itself. Additionally, the start of Israel's war in Gaza in October 2023 coincided with a massive increase in GPS spoofing incidents in the eastern Mediterranean Sea and Middle East. At the time of this report's publication, over twenty countries experienced endemic GPS interference over all or parts of their territories. That interference can include both GPS jamming and spoofing, as jamming a real GPS signal can make spoofing more effective.

Specifically, a jamming signal is broadcast at sufficient strength to overpower legitimate GPS signals, alongside a spoofing signal slightly more powerful than the jamming one, leading a GPS receiver to lock onto the spoofed signal. A spoofing signal is meant to appear like a legitimate GPS signal, but the spoofing signal transmits incorrect positional information. Though criminals,

Figure 3

TIMELINE OF NOTABLE GPS SPOOFING AND JAMMING ATTACKS

FEBRUARY 26, 2024

- The Norwegian Communication Authority reports an increase in spoofing and jamming incidents after the onset of the Russia-Ukraine war.

APRIL 2024

- California-based GPS developer oneNav conducts a field study, confirming "widespread Russian GPS jamming from Finland to Turkey." The company reports it has tested new technology designed to counter interference attacks in northern Israel.
- GPS jamming incidents increase in Lebanon, sparking protests in Beirut "over the threat to civil aviation."

MAY 2024

- Pilots flying over the Baltic Sea, the Black Sea, and the eastern Mediterranean report an increase in GPS disturbances, likely caused by Russian jammers.
- Due to cases of GPS interference, Finnish airline Finnair cancels daily flights to Tartu, Estonia, from April 29 to May 31, 2024.

MAY 29–JUNE 2, 2024

- Approximately 500 planes and hundreds of ships experience GPS issues due to North Korean interference.

AUGUST 2024

- A United Airlines flight from New Delhi to New York suffers a GPS spoofing attack originating in the Black Sea region. The attack compromises navigation systems for the rest of the flight.
- The number of flights affected by spoofing increases from "a few dozen in February to over 1,100 in August 2024."

OCTOBER 2024

- Approximately 1,000 flights per day report suffering from interference when flying over northern Israel and Ukraine.
- Finland's Coast Guard reports GNSS and GPS disturbances in the Baltic Sea, stating that "tankers were spoofing their location data to cover up visits to Russia."

OCTOBER 4, 2024

- South Korea reports 578 total instances of GPS interference between January and August.

NOVEMBER 8–9, 2024

- North Korean GPS interference impacts an unspecified number of flights and vessels for two days in a row, according to South Korean military officials.

DECEMBER 2024

- An increasing number of spoofing incidents are reported in Jordan, impacting roughly 244 flights.

JANUARY 17, 2025

- A Ryanair flight from London to Vilnius is diverted to Warsaw, Poland, due to GPS spoofing attacks near NATO's eastern border.

FEBRUARY 2025

- Pakistani airports report GPS signal interference, which impacts aircraft flying into and around the Karachi, Lahore, and Islamabad airports.

FEBRUARY 26, 2025

- The International Air Transport Association releases its 2024 Annual Safety Report, citing Türkiye, Iraq, and Egypt as GNSS interference hotspots and noting a 500% increase in GPS spoofing incidents between 2023 and 2024.

MARCH 2025

- Airlines report 465 instances of GPS interference and spoofing around Amritsar and Jammu between November 2023 and February 2025.
- Business aircraft crews report increased incidents of "GPS jamming and spoofing interference during international trips, especially in the Middle East."

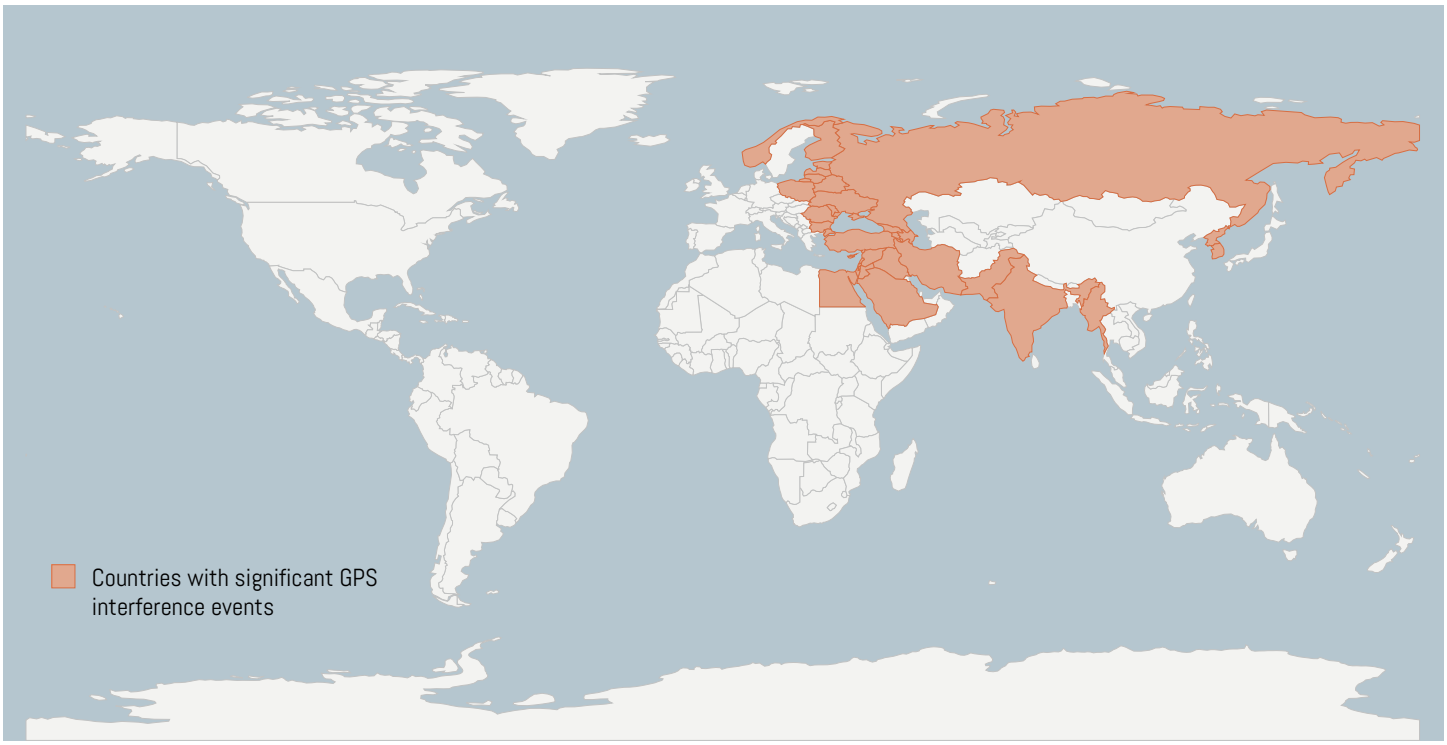
MARCH 26, 2025

- UN agencies issue a joint statement expressing "grave concern" about the rise of RNSS jamming and spoofing attacks.

ITU, *NEWSWEEK*, *BREAKING DEFENSE*, GPS WORLD, REUTERS, AND THE NATIONAL BUSINESS AVIATION ASSOCIATON

Figure 4

LOCATIONS OF SIGNIFICANT GPS INTERFERENCE EVENTS BETWEEN APRIL 2024 AND MARCH 2025



CSIS AEROSPACE SECURITY PROJECT RESEARCH AND ANALYSIS, ZHAW/SKAI DATA SERVICES USING OPENSKY NETWORK, AND GPSJAM.ORG

terrorists, and other nonstate actors may still find it easier to acquire and use GPS jammers, nation states that have access to powerful long-range electronic warfare capabilities have clearly found that spoofing can be more effective than jamming alone because GPS receivers often do not realize they are being spoofed but easily recognize when a GPS signal is blocked.

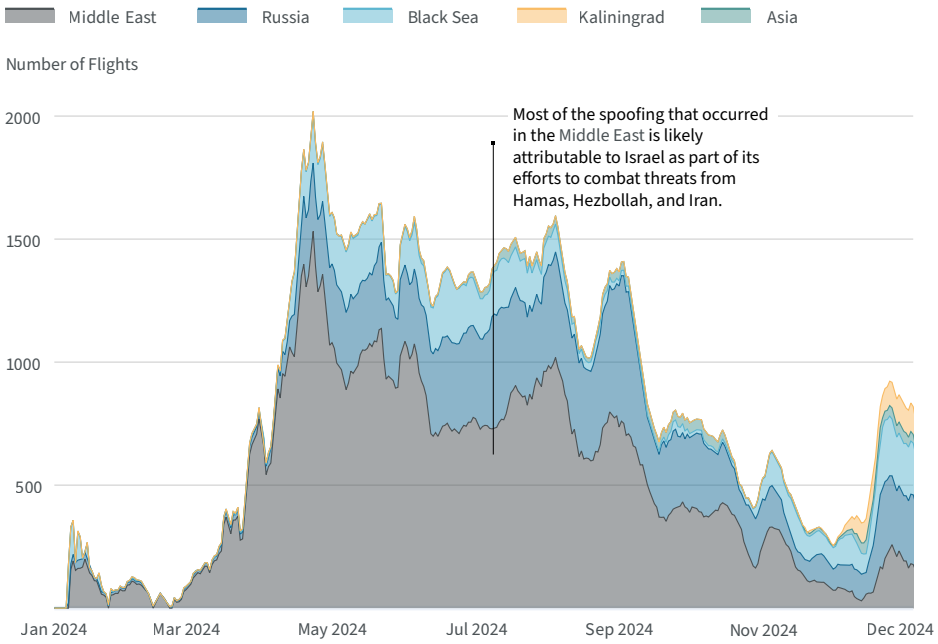
According to publicly available data, estimates for the number of worldwide commercial flights experiencing spoofing increased from 500 or fewer per day between January and mid-March 2024 to a peak of nearly 3,000 flights in April 2024, before leveling off at between 1,000 and 1,500 affected flights per day for the following several months.[11] Most of these spoofing incidents occurred in the Middle East and were likely attributable to Israel as part of its efforts to combat threats from Hamas, Hezbollah, and Iran. The greatest spike in spoofing incidents over the last year, in mid-April 2024, followed Israel's airstrike on April 1, 2024, targeting senior Iranian commanders in Syria, while Israel awaited possible Iranian retaliation, which ultimately came on April 13, 2024.[12]

Also, around April 2024, the Black Sea region and Russia experienced a surge in the number of flights daily reporting GPS spoofing, with these activities plausibly attributed to Russian efforts to defend against missiles and drones launched from Ukraine. This time frame coincides with a drone attack deep into Russia from Ukraine, a major drone attack on a Russian airbase, and stepped-up drone attacks on other important targets inside Russia.[13] Over the next several months, Ukraine continued to launch drone attacks on Russia, executing one of its largest drone strikes on Moscow in August 2024.[14] Up until early 2025, Ukraine had maintained a steady cadence of drone attacks on targets in Russia, likely prompting Russia to continue GPS jamming and spoofing as part of an integrated air defense campaign to defeat drones.[15] In August 2024, Ukraine destroyed an abandoned offshore gas platform in the Black Sea that Russia had been using for GPS spoofing operations, though it is not clear how the rig's destruction impacted Russia's spoofing capabilities.[16]

Outside of the Middle East, Russia, and Baltic and Black Sea regions, several other regions experienced significant GPS interference from January 2024 to April 2025, when this report was published.[17] These

Figure 5

DAILY NUMBER OF AFFECTED FLIGHTS PER SPOOFED-TO AREA



ZHAW/SKAI DATA SERVICES, USING OPENSKY NETWORK

areas include the region between Lahore, Pakistan, and New Delhi, India, particularly along the countries' shared border, and Myanmar. In Myanmar, GPS interference is a response by Myanmar's military to the rise in drone attacks carried out by armed groups affiliated with the opposition party in the country's ongoing civil war.[18] Some GPS spoofing was observed near the border between North Korea and South Korea throughout 2024, peaking around June.[19] There were also some reports of sporadic spoofing in Beijing in May 2024.[20]

To date, there are no indications that diplomatic pressure or condemnation has discouraged any nation state from deploying GPS jamming and spoofing systems in and around conflict zones or within their own national territories. Neither broad warnings from the International Telecommunication Union, the UN agency charged with facilitating international coordination on spectrum use, nor directed complaints from affected countries have altered Russia's behaviors.[21] Even though the International Civil Aviation Organization, the United Nations' civil aviation agency, admonished North Korea for repeatedly jamming GPS signals near its border with South Korea in May and June 2024, GPS interference was still being reported around the Korean Peninsula as of February 2025.[22] In spite of complaints about its efforts to disrupt GPS, Israel continues to spoof signals throughout the region, with the eastern Mediterranean region widely affected during the past year.[23]

THE DRIP-DRIP OF CYBERATTACKS

Continuing trends noted in past reports, there has been no shortage over the last year of cyberattacks targeting government, critical infrastructure, and other sectors, including space. But developing a way to accurately tally and characterize certain key aspects of cyberattacks, such as attacker motivations and objectives, is a challenge. The presence of a persistent cyber threat actor on a network may be discovered without revealing the hackers' aims, leaving questions about the actual target of the attack. For the authors of this report, this ambiguity makes it difficult to determine which cyberattacks qualify as attacks on space systems and related infrastructure and, thus, deserve attention in this report. For example, a threat actor might be detected on the servers of an academic research institute with an aerospace engineering department. Was this attacker targeting space systems (i.e., worth mentioning in a report on counterspace threats)?

Additionally, because some cyberattacks are only made public by the attackers with no confirmation from the victim organization, it can be difficult to understand the full impact of hacks or even know for certain whether an attack took place. Frequently, hackers publicly post screenshots or other evidence of a successful cyber exploit, to demonstrate data theft, to claim credit for the hack, or in the case of ransomware attacks, to pressure victims to comply with financial demands.[24] But hackers, particularly ones motivated by geopolitical or ideological aims, could also theoretically claim credit for attacks that never took place or exaggerate the scope of their exploits for propaganda purposes.

IT CAN BE DIFFICULT TO UNDERSTAND THE FULL IMPACT OF HACKS OR EVEN KNOW FOR CERTAIN WHETHER AN ATTACK TOOK PLACE.

Table 4

REPORTED CYBER INCIDENTS IN 2024 IMPACTING THE SPACE SECTOR

Attack Description	Source of Attack Disclosure	Affected Sectors
Unknown threat actors stole credentials of employees of 30 companies across various industries worldwide beginning in early July 2024.	Incident disclosed by IT-security company.	Energy, finance, government, health, space, and telecommunications
Unknown threat actors compromised the company network of Maxar Space Systems on October 4, 2024.	Incident disclosed by victim.	Space and critical manufacturing
Chinese-speaking threat cluster TIDRONE has targeted Taiwanese military and satellite industries with malware toolsets CXCLNT and CLNTEND since April 2024.	Incident disclosed by IT-security company.	Defense, space, and telecommunications
Iran-linked Peach Sandstorm used malware to backdoor Australian, UAE, and U.S. organizations between April and July 2024.	Incident disclosed by IT-security company.	Energy, government, and space
Pro-Ukrainian hacktivists BO Team targeted Russian State Research Center on Space Hydrometeorology, "Planeta," in January 2024.	Incident disclosed by government authorities.	Research and space

"EUROPEAN REPOSITORY OF CYBER INCIDENTS (ERCI)," GERMAN INSTITUTE FOR INTERNATIONAL AND SECURITY AFFAIRS, ACCESSED MARCH 24, 2025, HTTPS://WWW.SWP-BERLIN.ORG/EN/SWP/ABOUT-US/ORGANIZATION/SWP-PROJECTS/EUROPEAN-REPOSITORY-ON-CYBER-INCIDENTS-ERES POC.

Beyond the challenges in understanding hacker goals, positively identifying the physical location of hacker groups can be difficult. For example, experts do not yet know who is behind the IntelBroker hacker group, which has targeted aerospace related entities in the last year, with some indications it may be a lone-wolf actor from Serbia, and others that it might be affiliated with Iran.[25] This lack of clarity on affiliation and physical location of a hacker group complicates attribution, making it hard for the United States and other victims of attacks to calibrate their response to hacks. It also makes it difficult to predict where such hackers may strike next and who should be particularly on guard for attacks from mysterious groups like IntelBroker.

For all these reasons, the authors of this report have found it hard to count year-by-year the number of cyberattacks targeting space systems. Though their numbers differ, some organizations try to keep tallies of cyberattacks by the type of entity and sector targeted, among other criteria. According to the European Repository of Cyber Incidents (ERCI), a free database containing reports of worldwide cyberattacks, there were about 720 reported incidents across all sectors in 2024, with roughly 57 percent of incidents targeting critical infrastructure.[26] Of that total number, the database lists five attacks as specifically targeting the space sector in 2024, approximately the same number of attacks that targeted the space sector in 2023, according to ERCI.

The cyberattack documented by ERCI targeting Maxar Space Systems in October 2024 provides few insights into the motives or aim of the attackers.[27] At the time of discovery, hackers had only gained access to employee data on Maxar's networks. There is no public indication of whether personal information was the goal of the hack or whether gaining this limited access was the first step in a broader effort to breach operational or other systems specific to Maxar's satellites or space systems. The hackers may very well have been targeting Maxar because it is a space company, but it is equally plausible that Maxar's servers were just one IP address on a long list of unrelated entities, ones for which they merely found an exploitable vulnerability.

That there were only five reported cyber incidents affecting the space sector in 2024 according to the ERCI dataset may leave some readers of this report scratching their heads, as there is a widespread perception that space systems face constant cyber threats. In June 2024, the head of the Space Information Sharing and Analysis Center (Space ISAC)—a nonprofit organization set up in 2019 to improve threat sharing and mitigation for space systems and comprised of over 100 members across the public and private sectors within the United States and internationally—said that the organization records over 100 instances of cyberattacks targeting "infrastructure related to space systems" each week.[28] Though on the surface these numbers are clearly at odds with the rather low number of cyber incidents targeting the space sector according to the ERCI figures, the Space ISAC figures include attempted intrusions and hack claims made by attackers and not only, as the ERCI records report, successful attacks publicly acknowledged by hack victims. Additionally, the Space ISAC statistic speaks to the number of attacks targeting infrastructure related to space systems, which seems to include

Table 5

CYBERATTACKS IN 2024 IMPACTING THE SPACE SECTOR

Hacker Affiliation	Threat Actor Name(s)	Probable Threat Actor Motivation
Russia	Stormous, SpaceBears, NoName057(16), LockBit, Phoenix, and others	Data theft
China	TIDRONE, BianLian	Data theft
Iran	Peach Sandstorm, UNC1549	Data theft
North Korea	Andariel (Onyx Sleet), UNC2970	Data theft
Other or unknown	Anonymous Bangladesh (BD), SN BLACKMETA, IntelBroker, Sapphire Werewolf, and others	Data theft, financial gain (ransomware), politically motivated disruptions

DATA PROVIDED BY THE SPACE ISAC

more types of networks than are included in the term "space sector" used by ERCI.

In yet another attempt to tally cyberattacks targeting space systems, ETH Zurich, a Swiss university, published a report in October 2024 that documented over 120 publicly known cyber operations, between February 2022 and September 2024, targeting the space sector in the context of the war in Ukraine.[29] The report identified 12 pro-Ukrainian and 19 pro-Russian cyber threat actors who made claims to have targeted space systems. Of the attacks assessed in the report, the vast majority—65 percent—were distributed denial of service attacks, with 11 percent identified as network intrusions and 9 percent listed as leak operations. A further nine categories of hack types were specified in the report, including credential theft, data breach, malware, software cracking, and data breach extortion, among others.

One final observation is that, though the available data points to attempted and successful cyberattacks targeting systems associated with the space sector, there are no public reports in the last year that these cyberattacks have specifically targeted spacecraft or satellites in space. References to satellite hacking usually relate to attacks on ground infrastructure, the user terminal only, or the companies and institutions involved in satellite development and operations.[30] This does not mean that cyber threat actors have not compromised satellites in space, only that there is no open-source indication of such efforts in the last year.

RPOS: BENEVOLENT OR CRUEL INTENTIONS

Though space has never been a static environment—relative to the center of the Earth, the orbital speed of GEO satellites is 7,000 miles per hour and LEO satellites around 17,500 miles per hour—most spacecraft have generally tended to stay away from other space vehicles to avoid potential collisions. However, government-owned and commercial satellites are becoming more maneuverable and flying closer together, conducting rendezvous and proximity operations, or RPOs, and docking with other spacecraft on an increasingly regular basis. In 2024, there was strong private sector interest in developing satellites to perform maintenance, repair, assembly, manufacturing, and inspection missions. Government agencies continue to work on systems that use orbital maneuvering, RPO, and docking capabilities, such as space planes, crewed spacecraft, and scientific missions.[31] Additionally, no matter a satellite's specific function, it may need to maneuver to avoid collision with another satellite or a piece of space debris.

Given the variety of use cases for maneuvering one spacecraft around another, it can be difficult to characterize a spacecraft's purpose using only data about its behaviors in space. Some spacecraft exhibiting RPO behaviors may be counterspace weapons or testing technologies for use on such weapons. Other spacecraft may have peaceful reasons—or, at least, reasons that do not involve the use of a weapon—to move closer to another active satellite. A spacecraft may even have a non-hostile reason to conduct RPO and docking operations near a noncooperative space object, such as a defunct satellite or piece of space debris—this is the business case for companies like Astroscale and Clearspace. But a U.S. observer noting a Chinese or Russian satellite shadowing or moving closer to one of its own satellites would reasonably view that behavior as threatening. Chinese or Russian observers probably have the same reaction when a GSSAP satellite approaches their spacecraft.

The issue is that the United States and its allies rightly do not take Russian or Chinese statements about the purposes of maneuvering spacecraft at face value and find little assurances from Russian or Chinese assertions of peaceful intentions in space. But analyzing behaviors alone does little to clarify what their spacecraft are actually doing. Knowledge about a satellite's capabilities and context—for example, that it has a grabber arm or device capable of latching onto another satellite or that it "birthed" a smaller object in proximity to a U.S. government satellite—can help more fully assess the purpose of a satellite exhibiting RPO behaviors. Some of these satellites displaying RPO behaviors are probably designed as counterspace weapons, meaning they have capabilities intended to blind, jam, damage, or destroy other satellites. Other satellites are possibly performing a space surveillance mission or are testing on-orbit satellite servicing technologies.

Coincidentally, the U.S. government and U.S. companies are fielding more space systems aimed at some of these purposes. Broadly speaking, the U.S. Space Command (USSPACECOM) is increasingly focused on using satellites that are designed for frequent orbital maneuvering.[32] The Space Force operates GSSAP, whose purpose is to collect SSA data.[33] The Space Force is also investigating a next-generation constellation of scout satellites in GEO.[34] U.S. company True Anomaly is planning to operate its own satellites carrying out inspection operations, having launched its first and second missions in 2024.[35] Another company, HEO, is using sensors on satellites to collect data about other space objects in LEO, though HEO's approach is to use naturally occurring flybys rather than active maneuvering to obtain data.[36] Beyond near Earth, the Air Force Research Laboratory is developing two satellites designed to obtain SSA data from cislunar space.[37]

There are no indications that any of the aforementioned U.S. satellites are weapons, though their maneuvering signatures and behaviors may mirror those of on-orbit counterspace weapons. The perception that satellites like these are weapons could increase the risk of miscalculation, a risk compounded as more and more satellites are launched with missions that include orbital maneuvering. But some maneuverable satellites, including those operated by U.S. allies and some planned by the United States itself, are intended as counterspace weapons. France, for example, publicly stated in 2024 that it plans on building LEO satellites that can actively defend against attacks in space, having already announced plans for a similar GEO capability, called YODA, in 2021.[38] The Trump administration's January 2025 executive order on "The Iron Dome for America" (now Golden Dome) includes direction to develop and deploy space-based interceptors to defend the U.S. homeland against advanced missile attacks.[39]

Based on satellite behaviors alone, there is hardly a way to distinguish between a surveillance tool and a weapon, though arguably, the same satellite could perform both roles. Though the United States should view attempts to surveil its satellites by Russia and China with concern, it would undoubtedly respond with considerably more restraint to a surveillance satellite approaching one of its own satellites than a counterspace weapon exhibiting the same behaviors. Greater transparency and awareness about specific satellite capabilities is a possible way to delineate between a weapon and surveillance capability. But a lack of trust between the United States and its allies on one side and Russia and China on the other would impede efforts to increase transparency, since both sides likely mistrust each other's ability to be truthful about the purpose of their satellites. The U.S. Space Force is building up its space intelligence collection, analysis, and targeting to enable a deeper understanding of foreign capabilities and to support commanders' operational needs.[40] Meanwhile, researchers from LeoLabs, the University of Bern, and Maxar are developing characterization methods that combine radar measurements, information from ground-based optical telescopes, and non-Earth imagery data to provide new insights that can be used for assessing a spacecraft's purpose.[41]

Such a distinction between surveillance assets and weapons aids the United States and its allies in calling out unsafe, irresponsible, and escalatory behaviors, especially when adversaries target surveillance assets as they have done in other domains. For example, in 2019, Iran shot down an unarmed, unmanned U.S. Global Hawk surveillance aircraft operating over international waters, and both China and Russia continue to harass U.S. and allied airborne ISR assets operating in international airspace over the South China Sea and Black Sea, respectively.[42]

There is further danger in this lack of distinction and transparency. Given that the U.S. government and private sector, as well as allied nations and geopolitical competitors, operate satellites with space surveillance and SSA missions, considering maneuverable surveillance satellites as threats akin to counterspace weapons could expose U.S. satellites doing those missions to increased Russian and Chinese counterspace risks. In addition, grouping satellites with counterspace weapons into the same category as surveillance satellites will make it more difficult for spacecraft operators to identify and calibrate responses to real threats that could damage, degrade, or destroy their space systems. Grouping both types of space systems together also increases the risk of misunderstanding and miscalculation between geopolitical competitors in space.

At the same time, satellites conducting RPOs can still pose a security threat and safety hazard to others. For example, the revelation in March 2025 that PRC satellites had practiced "dogfighting" maneuvers in space should be concerning. The authors could imagine scenarios where adversary satellites maneuver against a target (like a U.S. government satellite) as to force it to move, expend fuel, and degrade its mission.

For these reasons, the authors of this report assert that satellites designed solely for obtaining SSA data or performing space surveillance roles should not be considered counterspace weapons but, understandably, satellites conducting RPOs without a clear understanding of capability and intent may still be viewed as threats depending on the circumstances. As in other domains, the United States, Russia, China, and other countries should eye warily but expect their adversaries and geopolitical competitors to conduct surveillance and intelligence collection against their space assets. Surveillance activities in space should not provoke the same reaction as deployment and use of actual counterspace weapons. Creating a public expectation that inspector or surveillance satellites are a hostile threat to be treated as weapons puts U.S. companies with business plans around doing those very same things more into the crosshairs of U.S. adversaries than they would likely already be.

There is no doubt that satellites conducting surveillance on other satellites to understand their purpose and capabilities serve

Table 6

CHINESE AND RUSSIAN SATELLITES EXHIBITING UNUSUAL BEHAVIORS BETWEEN JANUARY 2024 AND MARCH 2025

Satellite	Country	Timeline	Description
TJS-2	China	2024	Tracked maneuvering at 44 meters per second, which is unusually high and uses significantly more fuel than the more standard range of 0.5 to 1 meters per second
TJS-4	China	2024	Maneuvered to position itself between a U.S. space surveillance satellite and the Sun, creating shadows that potentially blocked the U.S. satellite from properly photographing TJS-4
TJS-10	China	May 16, 2024	TJS-10 came within 25 kilometers of another Chinese satellite in GEO, TJS-3, on May 16, 2024
SJ-25	China	January 2025	Entered a coplanar orbit with SJ-21, a satellite which in 2022 attached to and moved a defunct Beidou satellite from its position in GEO to a graveyard orbit, suggesting SJ-25 may intend to refuel SJ-21
TJS-3	China	January 2025	Moved to within one degree latitude of SJ-21, possibly suggesting a supporting role for TJS-3 in an upcoming refueling attempt
SY-12-02	China	November 2024	After travelling westward, it reached 17.3 degrees East (over central Europe) and changed direction to begin a new eastward journey
SY-12-01	China	September 2024	After travelling eastward, it reached 178.9 degrees East (over the Pacific Ocean) and changed direction to begin a new westward journey
SY-24C-01/02/03	China	January 2025	SY-24C-01, SY-24c-02, and SY-24C-03–conducted corkscrew maneuvers around SJ-6-05B, believed to be another technology demonstrator with potential signals collection capability
SY-24C-03 and SJ-6-05A	China	March 2025	SY-24C-03 and SJ-6-05A conducted rendezvous and proximity operations, with each satellite maneuvering and the closest approach distance less than one kilometer
Cosmos 2576	Russia	May 2024	Entered into a coplanar orbit with a U.S. government satellite, USA 314
Cosmos 2581	Russia	March 5, 2025	Cosmos 2581 and Cosmos 2582 have moved in formation, coming as close as 100 meters apart
Cosmos 2582	Russia		
Cosmos 2583	Russia	March 7, 2025	Passed as close as 0.5 kilometers to Cosmos 2581 and Cosmos 2582, but has yet to maneuver since reaching orbit
Luch (Olymp) 2	Russia	July 2024	May have come as close as 5 kilometers from Thor 7, a European communications satellite
Luch (Olymp) 2	Russia	January 2025	May have come less than 1 kilometers from Intelsat 1002, an international communications satellite

CSIS AEROSPACE SECURITY PROJECT RESEARCH AND ANALYSIS

a military and intelligence purpose. But they can also help to prevent misunderstandings, ensuring that decisionmakers can better discriminate between satellites that are weapons (i.e., threats) and ones that are not. They also can play an important role in space safety for both government and commercial space operators, helping to build a comprehensive picture of what is happening in the space environment and understand which satellites are truly counterspace weapons threats.

POINTS OF INSTABILITY: UNINTENTIONAL SPACE DEBRIS GENERATION

Several debris-fragment-generating events in space have taken place since the publication of the last *Space Threat Assessment*, though there is no indication that any of these were intentional or caused by counterspace weapons. Previous editions of this threat assessment have not specifically addressed accidental debris-causing incidents; however, this report will discuss them, as they have the potential to create geopolitical complications and instability. Catalogued and tracked debris fragments pose risks to space safety and, should debris produced by a satellite of one nation cause harm to satellites operated by other nations, can lead to increased international tensions. Debris-producing events that generate no public alarms, uncatalogued debris fragments, and inadequately characterized debris clouds create even more risks, adding an unnecessary and avoidable element of surprise to the calculus.

For inexplicable reasons, certain debris-causing incidents are widely covered in the media, while others go entirely under the radar, without widespread public coverage. Though USSPACECOM often makes public announcements of debris-generating events, it did not issue statements for all events in the last year. However, commercial SSA entities often make public announcements of such events, as will the Office of Space Commerce once its Traffic Coordination System for Space (TraCSS) is operational.[43] Additionally, it can sometimes take weeks if not months before the Space Force enters new debris fragments into Space-Track. In many cases, private sector SSA organizations announce they are tracking far more pieces of debris than are either announced by USSPACECOM or logged by Space Force in Space-Track. Especially when the debris-generating incident is caused by a spacecraft associated with the U.S. government, Russia's Vimpel space object catalog is sometimes updated to reflect new debris fragments quicker than Space-Track.[44]

DEBRIS-PRODUCING EVENTS THAT GENERATE NO PUBLIC ALARMS . . . CREATE EVEN MORE RISKS.

During the last year, USSPACECOM only publicly announced five debris-causing breakup events, yet this section describes eight such events.[45] Furthermore, for each event acknowledged by USSPACECOM, this report highlights the differences between the official Space-Track numbers of cataloged debris fragments, as well as the timeliness of their cataloging, and other space-object-tracking options. One reason for the discrepancies may relate to the Space-Track fidelity standards, which relate to how well an object is understood before it is or is not cataloged. But no matter the cause, delays and inconsistencies in adding debris fragments resulting from spacecraft breakups and energetic events to Space-Track create avoidable space safety risks and may affect the credibility of the United States in the eyes of other international partners during discussions on norms of behaviors and rules of the road for space activities.

Resurs-P1 (Russia): Russia's Resurs-P1 broke up on June 26, 2024. Launched in 2013, Resurs-P1 was a commercial remote sensing satellite in LEO that operated until 2021, when it was deactivated upon its replacement by Resurs-DK1. USSPACECOM noted that the breakup generated over 100 trackable debris fragments, while LeoLabs stated that it was tracking about 180 pieces of debris immediately after the event.[46] Though not confirmed, experts speculate the breakup was caused by improper or incomplete passivation efforts upon the retirement of the satellite in 2021. As of early March 2025, 18 pieces of debris were included in Space-Track. Due to the low altitude of the breakup, all other fragments have likely already decayed and

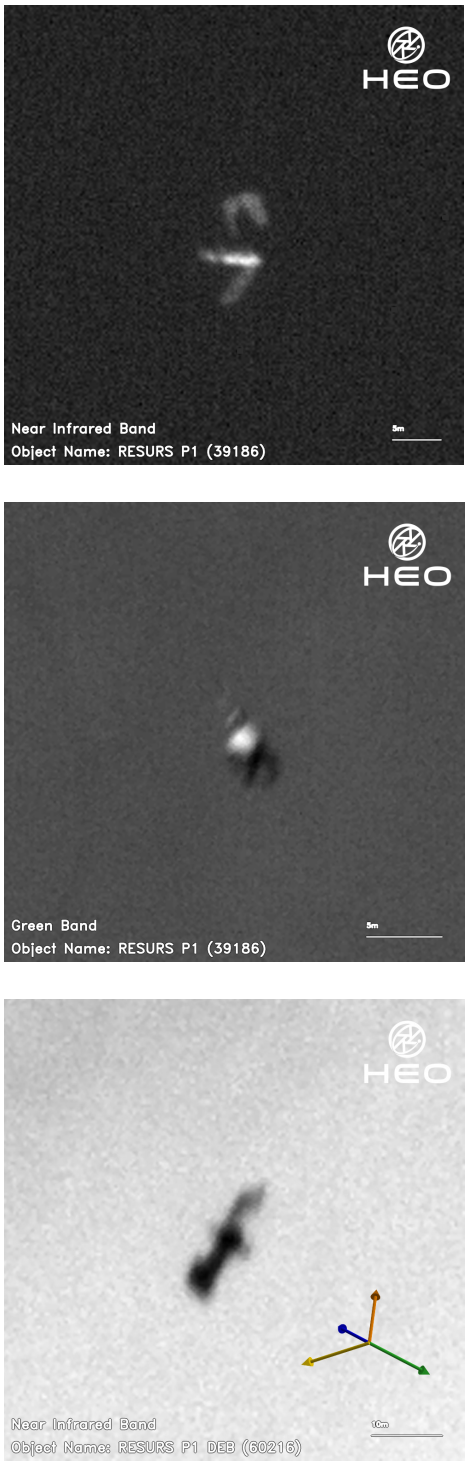
burned up in the atmosphere.

Upper Stage, Long March 6A (China): Most likely caused by residual propellant, the upper stage of a Long March 6A broke up in LEO, creating several hundred pieces of trackable debris—according to LeoLabs, potentially as many as 900 debris fragments—on August 6, 2024.[47] By early March 2025, over 650 fragments were logged in Space-Track. This rocket had been launched by China on that same day carrying satellites for the Qianfan ("Thousand Sails") LEO broadband satellite constellation. This was not the first time that the upper stage of a Long March 6A rocket broke up in orbit.[48]

Centaur Upper Stage, Atlas V (United States): On September 6, 2024, the Centaur upper stage of an Atlas V rocket broke up in a geotransfer orbit. The upper stage had been passivated after launching a U.S. government weather satellite in March 2018. As of early March 2025, Space-Track contained no debris fragments associated with this breakup, though an outside expert identified over 950 debris fragments by that time.[49] This is the fourth breakup of a Centaur upper stage, with two other breakups in 2018 and another in 2019. The cause of all four breakups is not known.

Intelsat IS-33e (United States): Intelsat IS-33e broke up on October 19, 2024, due to unknown reasons. Prior to the breakup, the satellite had been a telecommunications satellite in GEO, launched in 2016 with a planned service life of 15 years. Immediately following the breakup, USSPACECOM announced that it was tracking around 20 pieces of debris.[50] The number of debris fragments eventually reached at least 500, according to ExoAnalytic.[51] Space-Track, however, only listed 18 pieces of debris associated with this breakup event by early March 2025.

Defense Meteorological Satellite Program (DMSP) F-14 (United States): Probably due to a battery explosion, a defunct DMSP F-14 weather satellite in LEO generated a number of fragments on December 19, 2024.[52] Space-Track did not list any debris associated with this event by the end of December 2024, but both LeoLabs and Slingshot Aerospace were tracking debris fragments resulting from this event.[53] Since 2004, three other DMSP and two NOAA satellites using a similar design have all experienced similar malfunctions attributed to battery explosions. In early March 2025, Space-Track started listing debris from this satellite, with 19 fragments cataloged by March 10, 2025.



Photos of Resurs-P1 before and after the June 26, 2024, breakup event (top to bottom).

HEO

Blue Ring Pathfinder/Upper Stage, New Glenn (United States): Though not publicly reported by USSPACECOM, Blue Origin's New Glenn upper stage, to which the Blue Ring Pathfinder mission is attached, probably experienced a debris-generating event upon passivation in HEO on January 16, 2025.[54] Though originally thought to be ice and other effluent, which should have naturally dissipated, the debris fragments are probably a combination of thermal control materials and other unknown objects.[55] As of early February 2025, over 50 pieces of debris remained in orbit, with about 67 logged in Russia's space object catalog. As of March 2025, there are no debris fragments associated with this event in Space-Track.

Garpun 11L (Cosmos 2473) (Russia): On May 28, 2024, a nonoperational Russian military communications satellite in GEO, Garpun 11L (Cosmos 2473), experienced some kind of energetic event that raised the satellite 5 km and produced at least one new space object, identified in Russia's space object catalog.[56] Launched in September 2011, Garpun 11L has not been operational since experiencing an on-orbit malfunction in June 2020. USSPACECOM did not make any public announcements about this event and there is no indication of debris from this event in Space-Track as of April 2025.

Fregat RB/Cluster 2 Upper Stage, Soyuz-U (Russia): An experimental Russian upper stage, called Fregat RB/Cluster 2, of a Soyuz-U rocket launched in March 2000, experienced an energetic event on April 8, 2024, resulting in a 3-km change in the object altitude and some kind of residual propellant outgassing.[57] Though USSPACECOM has not provided a public notification of this event or listed any resulting debris fragments in Space-Track, the Russian space object catalog lists more than 300 pieces of debris generated by this event.[58] There is no indication of debris from this event in Space-Track as of April 2025.

THE COMING COLLISION OF COMMERCIAL AND COUNTERSPACE

Over the last decade, space has become increasingly commercial, and the past approach of sectioning space off into different military, civil, and commercial segments has become much more difficult. While space has traditionally been dominated by government activity and specialized defense contractors, the last decade has witnessed the growth of a diverse commercial space sector. Today, commercial companies act independently, with goals and actions to implement separate from government strategies or contracts.

In the rapidly advancing domain of space exploration and satellite technology, commercial space companies have become integral players, providing services ranging from satellite communication and Earth observation to space tourism and lunar exploration. As these companies expand their activities in LEO and beyond, they face an increasing risk of being caught in the crossfire of geopolitical tensions and the growing arms race in space. The impact of commercial space capabilities has been well documented in the war in Ukraine, where commercial services such as imagery and broadband communications were widely distributed in the early days and weeks of the conflict and largely continue today.

THE IMPACT OF COMMERCIAL SPACE CAPABILITIES HAS BEEN WELL DOCUMENTED IN THE WAR IN UKRAINE.

Governments around the globe have seen the impact that a space industrial base has on programs and economic bolstering, so commercial companies are being encouraged in most spacefaring nations to innovate alongside or outside of government priorities. The U.S. Department of Defense and Space Force have each released commercial integration strategies, and other nations around the globe are investing heavily in a commercial space sector, hoping to integrate innovative technologies into all facets of government capabilities. Multilateral organizations are also noting the importance of commercial capabilities, and NATO will reportedly publish a commercial space strategy in 2025.[59]

The rise of satellite companies offering critical services to governments, businesses, and individuals means that these private sector players are now directly in the crosshairs of geopolitical competitors and adversaries. As noted earlier in the report, in 2024, a Russian official indicated Russia would consider companies supporting U.S. "military space ambitions" as legitimate targets for retaliation."[60]

Beyond current capabilities such as communications or Earth imaging, commercial companies around the globe are testing technologies that could have counterspace applications. French company Dark plans to "forge the space armory" by building advanced defense systems to place on orbit to protect other satellites from being targeted.[61] Further, the Dark website states that space has already become a battlefield. The company is developing a platform called Interceptor, launched from a plane that would travel to LEO to move or deorbit satellites or pieces of debris. The company's CEO has described Dark as aiming to be the "S.W.A.T. team of space," and the Interceptor capability as ready to operate on call, akin to air defense missiles.[62]

Other technology developments are not as blunt, but could be considered a counterspace technology. Commercial companies are developing on-orbit servicing capabilities that are designed to extend an assets' life on orbit. But with capabilities like robotic arms and grapplers, these technologies have the potential for nefarious use. For example, Japanese company Astroscale is partnering with BAE Systems to test in-orbit servicing technology, in a contract funded by the European Space Agency to service a test satellite. The Astroscale satellite would do this servicing by conducting proximity operations to get close to the test satellite, then using a robotic arm to take a part off of the test satellite and replace it with a new part.[63] European space company Airbus, through its Surrey Satellite Technology Limited subsidiary, demonstrated a debris removal concept releasing a net and pencil-sized harpoon to capture space debris.[64] While the objective of these test missions is civil in nature, similar technologies could be used in the future for harming or disabling an adversary satellite.

The development of dual-use technologies, with both commercial and potential counterspace applications, underscores the delicate balance between actors in the space domain today. In an arena traditionally dominated by government agencies, private enterprises are now not only shaping the future of space exploration but also becoming entangled in geopolitical and security concerns. As these companies expand their capabilities and develop technologies that could have both peaceful and defensive applications, the lines between civilian, commercial, and military activities in space are becoming increasingly blurred.

WHAT TO WATCH

DISTINGUISHING BETWEEN PEACETIME NORMS AND WARTIME ACTIONS

Senior administration and Pentagon officials have repeatedly made clear that the U.S. military intends to be a responsible, good neighbor in space.[1] To meet that goal, the secretary of defense published a memo in 2021 outlining DOD tenets of responsible behavior in space.[2] Those tenets specify that DOD will operate in, from, to, and through space with due regard to others and in a professional manner; limit the generation of long-lived debris; avoid the creation of harmful interference; maintain safe separation and safe trajectory; and communicate and make notifications to enhance the safety and stability of the domain.

In February 2023, USSPACECOM proposed eight specific behaviors, which map to the five tenets, for DOD space operations, which USSPACECOM notes complement broader U.S. efforts to establish space norms and best practices.[3] Additionally, the United States has tried to discourage the testing of destructive DA ASAT weapons, which have the potential to generate space debris. In April 2022, the United States declared a moratorium on its testing of DA ASAT weapons. And in December 2022, along with several other nations, it introduced a UN resolution calling nations not to conduct destructive DA ASAT testing. The resolution was supported by over 150 countries.[4]

The tenets and eight behaviors are clearly applicable to day-to-day space operations and establish sensible norms for peacetime space activities, which apply to military space operations just the same as civilian and commercial ones. The moratorium on debris-generating destructive DA ASAT testing is a de facto peacetime restriction, as the preponderance of weapons testing would surely happen prior to a war or conflict. What is less clear is how these rules apply to wartime actions, though they have probably influenced the apparent U.S. emphasis on low-debris-causing and non-kinetic counterspace weapons, and how efforts oriented around space sustainability and safety, like the tenets, relate to the law of armed conflict.[5]

The general aims of the universal laws of war, including international humanitarian law, are to protect those not fighting and those no longer able to fight, which includes avoiding harm to civilians or things that are essential to their survival.[6] Though certainly open to interpretation, the operation of satellites in space is undeniably less essential than, and several steps removed from, the provision of things like food, water, medicine, and clothing to noncombatants. Except for humans on the International Space Station or China's Tiangong station, operations in space are unlikely to directly harm civilians. Operations on land, sea, and air are far more likely than those in space to harm people or cause disruptions to the delivery of the essentials of life. Yet the United States assigns the space domain a special set of tenets—though one-sided, since neither China nor Russia have agreed to these restrictions—for responsible behaviors that do not directly correlate to the expectations placed on combatants by the laws of war.

Rather than self-imposed tenets, applicable to one side and not the other, a better approach to space operations, particularly U.S. operations vis-à-vis China and Russia, could be one modeled on the 1971 agreement between the United States and Soviet Union on incidents on and over the high seas.[7] The goal of this agreement was not to cover wartime actions, but to prevent peacetime incidents from becoming more serious. The lessons from this approach for space operations are twofold. First, it could help establish norms of behavior for space that could improve overall space safety for military, civilian, and commercial operators. Second, it could help reduce the risk of misunderstanding between the United States, China, and Russia for space activities such as RPOs and other on-orbit behaviors.

This model also implicitly acknowledges that wartime actions are entirely different from peacetime behaviors, with guardrails placed around wartime behaviors established by the law of armed conflict, which is domain agnostic. Given the frequency of both Chinese and Russian RPOs and U.S. emphasis on space norms, a concerted U.S.-led effort over the next year to establish a space equivalent to the 1972 U.S.-Soviet agreement on incidents on and over the high seas would be beneficial both to U.S. interests and to the overall chances of success for the growth of the space economy.

MAKING MORE COUNTERSPACE WEAPONS PUBLIC

Historically, U.S. officials have shared little publicly about U.S. counterspace capabilities and operations. To date, the only publicly acknowledged counterspace weapons operated by the Space Force are the Counter Communications System and the Remote Modular Terminal, both electronic warfare capabilities.[8] The United States has emphasized these are defensive capabilities—not dissimilar from the use of GPS jammers and spoofers for force protection in Ukraine, Russia, and Israel described earlier—drawing a distinction between offensive and defensive space and emphasizing the U.S. intention to use space for deterrence and not aggression.[9]

In the next year, the United States may want to consider publicly revealing more, though not all, of its counterspace capabilities—as France and Germany are already doing—because acknowledging some U.S. counterspace weapons, beyond just jammers, can be used to deter hostile action in space or other domains.[10] Additionally, talking more publicly about counterspace weapons means the U.S. military can more easily partner with space companies already working on commercial technologies, such as servicing, debris removal, hypersonics, and atmospheric reentry, that could be transformed into new military space capabilities. For classified projects, the military also cannot tap into innovative space startups, as these companies often do not have the right security clearances to even know what the government wants to buy, let alone bid on the work.

THE UNITED STATES MAY WANT TO CONSIDER PUBLICLY REVEALING MORE, THOUGH NOT ALL, OF ITS COUNTERSPACE CAPABILITIES.

DEVELOPMENT OF BODYGUARD SATELLITES

As noted in this report, China has demonstrated it can operate highly maneuverable satellites in both LEO and GEO and track and synchronize orbits with U.S. government satellites. China also remains the only country to conduct a noncooperative capture of one satellite by another in GEO, when SJ-21 moved a defunct Beidou satellite into a graveyard orbit in 2022. These capabilities should be seen as ominous signs of the potential for China to develop, if it has not already done so, sophisticated on-orbit counterspace weapons against which U.S. satellites have limited, if any, defenses.

To date, France is the only country that has consistently talked about building and deploying on-orbit satellite systems designed to guard, defend, and protect high-value satellites. However, in May 2024, the European Commission announced that the European Defense Fund included €6.5 million ($7 million) for an "Autonomous SSA Bodyguard Onboard Satellite" that would perform SSA and threat detection, but also "counteract [threats] with a robot or laser."[11] It remains to be seen how the public acknowledgment of such initiatives will influence counterspace weapons trends, though one likely response from countries like China and Russia would be to develop new counterspace systems. This cat-and-mouse game between offensive and defense space capabilities will likely make space operations more expensive for both government and commercial operators, as space operators will likely want to invest in systems and methods that protect their space assets. It will also raise questions about what commercial operators are legally allowed to do to protect their satellites, similar to the issues raised in cyberspace about whether cyberattack victims can "hack back" against their attackers.

Looking to the future, the United States and its allies, beyond just France, will want new on-orbit technologies—like bodyguard satellites—to protect against on-orbit counterspace threats. Such systems could employ non-kinetic weapons, such as jammers and lasers, or kinetic weapons, such as projectiles or grappling capabilities, to disable attacking satellites. There is no reason to delay efforts to develop such capabilities and no reason to make such efforts secret.

GENERATION OF DEBRIS FRAGMENTS

Though experts frequently warn of increased risks of collisions and creation of space debris resulting from the deployment of large satellite constellations, most debris-generating incidents over the past year have nothing to do with operating satellite constellations. Of the eight debris-causing events described earlier in this report, only one involves an active satellite (e.g., Intelsat IS-33e). Further, while concern has focused on the risk of collisions in congested LEO orbits, only one related to LEO constellations, and even that connection is tangential because the event relates to the launch vehicle, the Long March 6A upper stage, and not the satellites themselves. Additionally, most of these events were caused by defunct spacecraft that were at least 10 years old, or rocket bodies.

Just as the operation of large satellite constellations to date has not caused a commensurate rise in space debris, neither has testing or use of kinetic counterspace weapons. Most debris from the U.S. military's shoot down of a defunct U.S. satellite in 2008, called Operation Burnt Frost, deorbited within days.[12] Additionally, the Russian ASAT test in 2021 created around 1,800 catalogued debris fragments, yet only around 9 tracked pieces remained in orbit by March 24, 2025, according to Space-Track.[13] The glaring exception is China's test of a DA ASAT in 2007. Because of the altitude of that test, around 800 km, nearly 70 percent of resulting debris remains in orbit.[14]

Though not directly related to the operation of large constellations, one trend to watch is China's tendency to date of leaving the upper stages of Long March 6A and 8 rockets used to launch its LEO broadband constellations at altitudes near 800 km. At that altitude, the rocket bodies could remain in orbit for more than 100 years, creating increased collision risks and the potential for debris-generating collisions or other events.[15] With plans to launch thousands of satellites for these constellations, unless China takes a different tack in the future, the risks from these rocket bodies will grow.

The fact is that most space debris fragmentation events result from breakups involving old satellites and incidents involving spent rocket bodies. These objects are ticking time bombs, which have a tendency to regularly and spectacularly go off, creating the vast majority of debris-generating incidents since the publication of last year's threat assessment. But so far, little is being done by the United States or other countries, including China and Russia, to address these main causes of increasing space debris. Though most breakup events are not caused by nefarious acts, debris-generating breakups pose just as much risk to the space environment as the counterspace weapons regularly chronicled in this report, and debris-generating breakups will continue to do so in the future.

MOST DEBRIS-GENERATING INCIDENTS OVER THE PAST YEAR HAVE NOTHING TO DO WITH OPERATING SATELLITE CONSTELLATIONS.

COUNTERING PROLIFERATED SATELLITE CONSTELLATIONS

The alarming news of 2024—that Russia is pursuing a space-based nuclear anti-satellite weapon—brought the first signs of active development, including on-orbit testing, of a counterspace weapon believed to be designed to counter proliferated LEO (pLEO) constellations en masse.[16]

Governments and commercial operators alike have embraced pLEO constellations: from first-mover Starlink, to the U.S. government through its investment in hundreds of satellites for ISR and missile detection and tracking, to China and its ISR and SATCOM system expansion. These architectures offer clear advantages: enhanced persistence, higher technology refresh rates, lower per unit costs, and greater resilience. Russian efforts to interfere with Starlink in Ukraine have been largely stymied by the sheer number of satellites still able to connect with ground terminals and SpaceX's ability to rapidly update its systems.

However, no advantage is permanent and, as previous editions of this report have cautioned, adversaries will seek new methods to erode it. Both this report and previous ones have drawn attention to PLA-affiliated research into attack simulations that could wipe out planes of LEO satellites, cyber penetrations of satellite networks and infrastructure that could impact satellite command and control, and high-altitude nuclear detonation (HAND) effects on satellites.[17] Further, Moscow is signaling new redlines with threats that commercial satellites, like Starlink, supporting military operations are legitimate targets.[18]

The authors fully expect to see more counter-pLEO threats in the years to come, a reminder that proliferation is but one means of enhancing resilience. The United States must figure out how to deter and defend against such attacks and minimize their catastrophic potential. At the same time, as countries like China utilize pLEO constellations to close their own "space-enabled kill chains," the United States will also seek ways to erode their capabilities.[19] The distinction for Washington will be to do so in ways that do not lay waste to orbits for all who use them to advance commerce, science, and security in contrast to Moscow's approach and even those hinted by Beijing.

SPACE AND MISSILE DEFENSE NEXUS

While this report does not describe U.S. counterspace weapons, it is impossible to ignore the counterspace implications of the "Golden Dome" missile defense initiative announced by the White House in January 2025. Specific details remain scarce, but the executive order points to the centrality of space for missile defense—encompassing space-based sensors for missile detection and tracking, data relay networks, and renewed interest in space-based interceptors (SBIs).[20]

Historical analyses suggest that thousands of SBIs in low Earth orbit would be necessary to intercept ballistic missiles in their boost phase, before countermeasures or maneuverable reentry vehicles are released.[21] These SBIs are certain to become high value counterspace targets. Russian officials have already accused the United States of undermining "Russian and Chinese strategic deterrence capabilities" with its Golden Dome plans.[22] Adversaries may well gravitate to nuclear ASATs or other wide area-effects weapons to neutralize such orbiting systems at scale.

Furthermore, though intended as a missile defense system, SBIs also have utility as counterspace weapons. An SBI equipped with a kinetic payload, laser, or microwave device could be used as a bodyguard satellite or to degrade an adversary's space systems. It also could be used to entirely cut off access to space, as it could be capable of destroying any attempted space launch withing minutes of a rocket leaving the launch pad, challenging an adversary's ability to reconstitute satellite systems damaged in a conflict. Taking a step further, SBIs may very well open the door to a broader conversation among policymakers on how to unlock the full military potential of the space domain for warfighting, including capabilities that operate "in, from, and through" space.[23]

CONCLUSION

"The years teach much which the days never know."

— RALPH WALDO EMERSON FROM ESSAYS: SECOND SERIES, 1844

THAT THIS REPORT CHRONICLES NO NEW SPECTACULAR COUNTERSPACE DEVELOPMENTS does not mean nothing interesting or noteworthy happened. To understand the events, and the significance, of this past year, one must look at the trends over a wider time horizon. Doing so reveals patterns that illuminate the direction of U.S. adversaries, as well as of the United States and its allies in space. China and Russia, as well as, to a lesser degree, Iran and North Korea, are actively working to test new technologies and concepts of operations in space that have clear applicability and use for counterspace weapons capabilities. Meanwhile, building on trends noted in past years, jamming and spoofing GPS signals has become ubiquitous in certain regions of the world, and cyber operations targeting space systems continue to take place and are uncovered on a regular basis.

To date, the United States has not publicly revealed its own counterspace-specific capabilities beyond two electronic warfare capabilities. Of its allies, only France has routinely acknowledged its intent to develop on-orbit counterspace capabilities that could perform defensive and offensive missions. From what is publicly known, the United States and its allies appear to be developing a much narrower range of counterspace weapons than their potential adversaries. This imbalance is possibly attributed to the commonly held assumption that the use of kinetic counterspace weapons in conflict is incompatible with maintaining a usable space environment for military space operations and somehow in conflict with the law of war. But the United States is reevaluating these assumptions, talking about kinetic counterspace weapons and space-based missile interceptors as part of the Golden Dome initiative.[1]

Ultimately, Russia and particularly China are demonstrating sophisticated counterspace capabilities in orbit, as well as deploying cyber and electronic warfare capabilities targeting space systems. Iran is growing more capable in space, deploying more satellites and having greater success with indigenous space launch capabilities. The United States has, to date, constrained its counterspace emphasis to non-kinetic capabilities and publicly expressed no interest in developing bodyguard satellites or other systems to defend against attacking satellites in space. But the United States is shedding those restraints.[2] Additionally, the secrecy that surrounds U.S. counterspace capabilities has to date limited its usefulness for deterrence purposes. In this complicated and increasingly threatening space environment, to retain its edge in space, the United States will need all the counterspace tools it can get its hands on, including bodyguard-style satellites. It should also be more public about the U.S. arsenal, ensuring that these systems can be used to the maximum extent for deterrence as well as warfighting.

ABOUT THE AUTHORS

CLAYTON SWOPE is the deputy director of the Aerospace Security Project and a senior fellow in the Defense and Security Department at the Center for Strategic and International Studies (CSIS). Before joining CSIS, Swope led national security and cybersecurity public policy for Amazon's Project Kuiper, an initiative to increase global broadband access through a constellation of satellites in low Earth orbit. While at Amazon, he also worked on cloud policy issues. Prior to his time at Amazon, Swope served as a senior adviser on national security, space, foreign affairs, and technology policy issues for a member of the U.S. House of Representatives. He also worked for more than 14 years at the Central Intelligence Agency, serving largely in the Directorate of Science and Technology. He holds a Bachelor of Science in mechanical engineering from the University of Notre Dame.

KARI A. BINGEN is the director of the Aerospace Security Project and a senior fellow in the the Defense and Security Department at CSIS. Before joining, she was the Chief Strategy Officer at HawkEye 360, an innovative space technology company. She previously served as the deputy undersecretary of defense for intelligence and security, overseeing the nation's defense intelligence and security enterprises. Prior, Kari was the policy director on the House Armed Services Committee and staff lead for its Strategic Forces Subcommittee, advising members of Congress on defense policy, program, and budget matters. Prior to government service, she worked in the national security space sector, supporting U.S. defense and intelligence community organizations. In addition to her work at CSIS, Kari is an adjunct assistant professor at Georgetown University. She is a member of the U.S. National Intelligence University's Board of Visitors, a member of the U.S. Strategic Command Strategic Advisory Group, and serves on a number of corporate and nonprofit advisory boards. She holds a degree in aeronautics and astronautics from the Massachusetts Institute of Technology.

MAKENA YOUNG is a fellow with the Aerospace Security Project at CSIS. Her research interests include international collaboration, space security, and orbital debris. Prior to joining CSIS, Ms. Young worked for the Federal Aviation Administration as an aerospace engineer, focusing on automatic dependent surveillance-broadcast certification and integration in small aircraft. She holds a BS in aeronautical and astronautical engineering from Purdue University with minors in international relations and environmental engineering.

KENDRA LAFAVE is a program coordinator and research assistant with the Aerospace Security Project at CSIS. She previously served as a program coordinator with the Hess Center for New Frontiers at CSIS. Prior to her time at CSIS, Kendra worked at the U.S. Civilian Research and Development Foundation (CRDF) Global and interned with the U.S. Department of State's Office of Peacekeeping Operations. Kendra graduated summa cum laude with a BA in international affairs from James Madison University. She is currently pursuing an MA in international science and technology policy from George Washington University, concentrating in space policy.

ENDNOTES

INTRODUCTION

1 Dan De Luce, "Pentagon official warns Russian anti-satellite nuclear weapon could be devastating," NBC News, May 1, 2024, https://www.nbcnews.com/news/world/pentagon-official-warns-russian-anff ti-satellite-nuclear-weapon-devastat-rcna150314.

2 Matt Burgess, "The Dangerous Rise of GPS Attacks," *Wired*, April 30, 2024, https://www.wired.com/story/the-dangerous-rise-of-gps-attacks/.

3 Zachary Cohen and Oren Liebermann, "Pentagon is closely monitoring Russia and China test military capabilities in space," CNN, March 16, 2025, https://edition.cnn.com/2025/03/16/politics/pentas gon-monitoring-russia-china-space/index.html.

4 Dmitry Antonov, Felix Light, and Guy Faulconbridge, "Russia warns United States: use of SpaceX for spying makes its satellites a target," Reuters, March 20, 2024, https://www.reuters.com/world/russia-warns-united-states-use-spacex-spying-makes-its-satellites-target-2024-03-20/.

5 Secretary of the Air Force Public Affairs, "Saltzman outlines Space Force priorities, what's necessary to achieve them," U.S. Space Force, March 13, 2025, https://www.spaceforce.mil/News/Article-Display/Article/4093782/saltzman-outlines-space-force-priorities-whats-necessary-to-achieve-them/; and "A Conversation with Secretary of the Air Force Frank Kendall on The Department of the Air Force in 2050," CSIS, January 13, 2025, https://www.csis.org/analysis/conversation-secretary-air-force-frank-kendall-department-air-force-2050.

COUNTERSPACE WEAPONS

1 Antonia Chayes, "Rethinking Warfare: The Ambiguity of Cyber Attacks," Harvard Law School, *Harvard National Security Journal*, no. 6 (June 2015): 474–519, https://harvardnsj.org/wp-content/uploads/2015/06/Chayes.pdf.

2 Space situational awareness (SSA) generally refers to the "knowledge and characterization of space objects and their operational environment" as defined in U.S. Space Policy Directive-3, National Space Traffic Management Policy, The White House, June 18, 2018, https://trumpwhitehouse.archives.gov/presidential-actions/space-policy-directive-3-national-space-traffic-management-policy/.

CHINA

1 Kristin Burke, "China Can Track GSSAP," China Aerospace Studies Institute, September 9, 2024, https://www.airuniversity.af.edu/CASI/Display/Article/3891422/china-can-track-gssap/.

2 Andrew Jones, "China to debut new Long March and commercial rockets in 2025," *SpaceNews*, January 2, 2025, https://spacenews.com/china-to-debut-new-long-march-and-commercial-rockets-in-2025/.

3 Andrew Jones, "China nears record launch year with Ceres-1 and SAR satellite missions," *SpaceNews,* December 19, 2024, https://spacenews.com/china-nears-record-launch-year-with-ceres-1-and-sar-satellite-missions/.

4 Theresa Hitchens, "China's space moves: Highly mobile satellites stalking GEO spook Space Force," *Breaking Defense*, December 10, 2024, https://breakingdefense.com/2024/12/chinas-space-moves-highly-mobile-satellites-stalking-geo-spook-space-force/.

5 Guy Norris, "Concerns Grow Over Chinese Space Maneuvering Capability," Aviation Week, August 21, 2024, https://aviationweek.com/defense/concerns-grow-over-chinese-space-maneuvering-capability; Greg Hadley, "China's Orbital Maneuvers Have Space Force Leaders Seeking Better Options," *Air and Space Forces Magazine*, December 11, 2024, https://www.airandspaceforces.com/china-space-force-maneuver/; and "Integrity Flash: Analysis of Developments in the Space Domain, Issue 104," Integrity ISR, September 1, 2024, https://isruniversity.com/wp-content/uploads/2025/02/integrity-flash-104.pdf.

6 "Integrity Flash: Analysis of Developments in the Space Domain, Issue 104," Integrity ISR.

7 “TJS-3 and TJS-10: Space Events May 2024,” LSAS Tec, YouTube video, June 17, 2024, https://www.youtube.com/watch?v=mTVacnXslpE.

8 Andrew Jones, “China Launches Shijian-25 Satellite to Test On-Orbit Refueling and Mission Extension Technologies,” *SpaceNews*, January 6, 2025, https://spacenews.com/china-launches-shijian-25-satellite-to-test-on-orbit-refueling-and-mission-extension-technologies/.

9 Greg Gillinger (@Integrity ISR), “Fill ‘Er Up? Shijian-25 Launched, Co-Planar with Shijian-21: Integrity Flash-Lite 8,” LinkedIn, January 16, 2025, https://www.linkedin.com/pulse/fill-er-up-shijian-25-launched-co-planar-shijian-21-integrity-yxw8e/.

10 “Integrity Flash: Analysis of Developments in the Space Domain, Issue 113,” Integrity ISR, January 19, 2025, https://isruniversity.com/wp-content/uploads/2025/02/113-19-Jan-2025-Integrity-Flash.pdf.

11 A report published in March 2022 by the China Aerospace Studies Institute draws a distinction between the purpose of the SY and SJ programs, assessing that the SJ program aims to operationalize systems that have already been integrated and tested, while the SY program’s goal is to integrate new technologies into one satellite system, see Kristin Burke, “Initial Analysis of Two Chinese Satellite Series: Shi Jian and Shi Yan,” China Aerospace Studies Institute, March 28, 2022, https://www.airuniversity.af.edu/CASI/Display/Article/2975081/initial-analysis-of-two-chinese-satellite-series-shi-jian-and-shi-yan/.

12 China Aerospace News, “刚才！长七A海南起飞 [Just Now! Chang-7A Hainan Take-Off],” Weibo.cn, December 23, 2021, Translated by Microsoft Translator, https://m.weibo.cn/status/L7oUgqkaZ.

13 “Integrity Flash: Analysis of Developments in the Space Domain, Issue 111,” Integrity ISR, December 8, 2024, https://isruniversity.com/wp-content/uploads/2025/02/111-8-Dec-2024-Integrity-Flash.pdf.

14 “Integrity Flash: Analysis of Developments in the Space Domain, Issue 105,” Integrity ISR, September 15, 2024, https://isruniversity.com/wp-content/uploads/2025/02/105-15-Sep-2024-Integrity-Flash.pdf.

15 Slingshot Aerospace, “The Slingshot Global Sensor Network is tracking a new object in low Earth orbit (LEO),” LinkedIn, May 29, 2024, https://www.linkedin.com/posts/slingshot-aerospace_the-slingshot-global-sensor-network-is-tracking-activity-7201624236233289729-Z3rF; and Andrew Jones, “China’s Secretive Reusable Spaceplane Lands after 267 Days in Orbit,” *SpaceNews*, September 6, 2024, https://spacenews.com/chinas-secretive-reusable-spaceplane-lands-after-267-days-in-orbit/.

16 Andrew Jones, “China Launches Mystery Reusable Spaceplane for Third Time,” *SpaceNews*, December 14, 2023, https://spacenews.com/china-launches-mystery-reusable-spaceplane-for-third-time/.

17 “Integrity Flash: Developments and Analysis in the Space Domain, Issue 113” Integrity ISR; and Justin Davenport, “Long March 4B with Shijian-6 Group 5 satellites launches successfully from Jiuquan,” NASA Spaceflight, December 9, 2021, https://www.nasaspaceflight.com/2021/12/long-march-4b-shijian-6/.

18 s2a systems (@s2a_systems), “For one of our clients (thanks for permission to share the information) we are currently taking a closer look at SHIYAN 24C 03 (2023-206C/58652) and SHIJIAN 6 05A (2021-122A/49961),” X, April 20, 2024, 1:38 a.m., https://x.com/s2a_systems/status/1781558085376491710.

19 Simone McCarthy, “China is practicing ‘dogfighting’ with satellites as it ramps up space capabilities: US Space Force,” CNN, March 21, 2025, https://edition.cnn.com/2025/03/21/china/china-space-force-dogfighting-satellites-intl-hnk/index.html.

20 Kristin Burke, “China’s Different Approach to Space Situational Awareness,” China Aerospace Studies Institute, December 2, 2024, https://www.airuniversity.af.edu/CASI/Display/Article/3980318/chinas-different-approach-to-space-situational-awareness/.

21 Ibid.

22 Ibid.

23 LSAS Tec (@LSAS-Tec), “Check out the intriguing interactions between USA LDPE-3A and China’s SJ-23 satellites in GEO during late 2024,” LinkedIn, February 2025, https://www.linkedin.com/posts/lsas-tec_spaceanalysis-geo-satelliteinteraction-activity-7292584494052564994-9oBK; and “Next Space Force payload arrives in Florida ahead of January 2023 launch,” media release, U.S. Space Systems Command, November 14, 2022, https://www.ssc.spaceforce.mil/Portals/3/Documents/PRESS%20RELEASES/Next%20Space%20Force%20payload%20arrives%20in%20Florida%20ahead%20of%20January%202023%20launch.pdf?ver=a9Bcr8my-xTYIYzVnCuMEw%3D%3D.

24 Joel Francis, "Briefing 29: Implications of the Ongoing Salt Typhoon Campaign on Telecommunications and Space," Constellations, January 15, 2025, https://www.kratosdefense.com/constellations/articles/implications-of-the-ongoing-salt-typhoon-campaign-on-telecommunications-and-space.

25 Cybersecurity and Infrastructure Security Agency et al., "Joint Cybersecurity Advisory: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," U.S. Department of Defense, February 7, 2024, https://media.defense.gov/2024/Feb/07/2003389935/-1/-1/0/CSA-PRC-COMPROMISE-US-CRITICAL-INFRASTRUCTURE.PDF; and Josh Hanrahan, "VOLTZITE Espionage Operations Targeting U.S. Critical Systems," Dragos, Inc. February 2024, https://hub.dragos.com/hubfs/116-Datasheets/Dragos_IntelBrief_VOLTZITE_FINAL.pdf?hsLang=en.

26 Pierre Lee and Vickie Su, "TIDRONE Targets Military and Satellite Industries in Taiwan," Trend Micro, September 6, 2024, https://www.trendmicro.com/en_us/research/24/i/tidrone-targets-military-and-satellite-industries-in-taiwan.html.

27 GPS Spoofing WorkGroup, *GPS Spoofing: Final Report of the GPS Spoofing WorkGroup* (OPSGROUP, September 2024), https://ops.group/blog/gps-spoofing-final-report/.

28 Defense Intelligence Agency, *Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion* (Washington, DC: Defense Intelligence Agency, 2022), https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf.

29 Andrew Jones, "China reorganizes its military, impacts likely for space operations," *SpaceNews*, April 23, 2024, https://spacenews.com/china-reorganizes-its-military-impacts-likely-for-space-operations/; and "The Ministry of National Defense held a special press conference on the establishment of the Information Support Force," Xinhua Daily Telegraph, April 20, 2024, http://www.news.cn/mrdx/2024-04/20/c_1310771952.htm.

30 Stephen Chen, "China's energy weapon fires thousands of intense pulses in tests and survives: study," *South China Morning Post*, January 14, 2025, https://www.scmp.com/news/china/science/article/3294077/chinas-energy-weapon-fires-thousands-nuclear-blasts-tests-and-survives-study; and Stephen Chen, "China could attack Starlink-like satellites with submarine laser weapon: naval study," *South China Morning Post*, January 14, 2025, https://www.scmp.com/news/china/science/article/3294077/chinas-energy-weapon-fires-thousands-nuclear-blasts-tests-and-survives-study/.

31 Clayton Swope et al., *Space Threat Assessment 2024* (Washington, DC: CSIS, April 2024), https://www.csis.org/analysis/space-threat-assessment-2024; and "Space Threat Fact Sheet," Headquarters Space Force Intelligence, February 21, 2025, https://www.andrewerickson.com/2024/09/headquarters-space-force-intelligence-space-threat-fact-sheet/.

32 Du Yanyun and Zhang Huang, "Starlink Militarization and Its Impact on Global Strategic Stability," *Interpret: China*, CSIS, original work published in *Journal of International Security Studies*, September 19, 2023, https://interpret.csis.org/translations/starlink-militarization-and-its-impact-on-global-strategic-stability/; Yan Jiajie and Yu Nanping, "The U.S. Starlink Project and Its Implications from the Perspective of International and National Security," *Interpret: China*, CSIS, original work published in *Journal of International Security Studies*, September 14, 2024, https://interpret.csis.org/translations/the-u-s-starlink-project-and-its-implications-from-the-perspective-of-international-and-national-security/; and Wang Peiwen, Zhang Huang, and Zhang Kaiyue, "Starlink Militarization: Challenges and Responses to Space Intelligence and Information Security," *Interpret: China*, CSIS, original work published in *Journal of Intelligence*, January 29, 2024, https://interpret.csis.org/translations/starlink-militarization-challenges-and-responses-to-space-intelligence-and-information-security/.

33 Brian Weeden, Cassandra Steer, and Fiona Cunningham, "Chinese Assessments of Starlink and U.S.-China Space Relations," CSIS, *Interpret: China*, December 2, 2024, https://interpret.csis.org/chinese-assessments-of-starlink-and-u-s-china-space-relations/.

34 "Is China Planning to Target Starlink Satellites Amid Taiwan Tensions?," *Economic Times*, January 14, 2025, https://economictimes.indiatimes.com/news/international/us/is-china-planning-to-target-starlink-satellites-amid-taiwan-tensions/articleshow/117245640.cms.

35 "Chinese scientists simulate 'hunting' Starlink satellites in orbit," *South China Morning Post*, January 12, 2025, https://www.scmp.com/news/china/science/article/3294047/chinese-scientists-simulate-hunting-starlink-satellites-orbit.

36 "Foreign Universities Sanctioned by the U.S. Government," Caltech Offices of Research Compliance and Security, last updated January 16, 2024, https://researchcompliance.caltech.edu/compliance/ex/

port-compliance/restricted-party-screening/foreign-universities-sanctioned-by-the-us-government; and Rachel Lin and Jonathan Chin, "Seven Chinese universities sanctioned," *Taipei Times*, March 1, 2025, https://www.taipeitimes.com/News/front/archives/2025/03/01/2003832691.

RUSSIA

1 House Intelligence Committee (@HouseIntel), "Statement from Chairman @RepMikeTurner:", X, February 14, 2024, 11:35 a.m., https://x.com/HouseIntel/status/1757805804885823775; Jacob Parkinson et al., "GOP warning of 'national security threat' is about Russia wanting nuclear weapon in space: Sources," ABC News, February 14, 2024, https://abcnews.go.com/Politics/white-house-plans-brief-lawmakers-house-chairman-warns/story?id=107232293; and Michael Williams and Kevin Liptak, "White House confirms US has intelligence on Russian anti-satellite capability," CNN, February 15, 2024, https://www.cnn.com/2024/02/15/politics/white-house-russia-anti-satellite/index.html.

2 "Pentagon Press Secretary Air Force Maj. Gen. Pat Ryder Holds a Press Briefing," U.S. Department of Defense, May 21, 2024, https://www.defense.gov/News/Transcripts/Transcript/Article/3783786/pentagon-press-secretary-air-force-maj-gen-pat-ryder-holds-a-press-briefing/.

3 Slingshot Aerospace (@Slingshot-Aerospace), "The Slingshot Global Sensor Network is keeping a close watch on Cosmos 2576," LinkedIn, May 2024, https://www.linkedin.com/posts/slingshot-aerospace_the-slingshot-global-sensor-network-is-keeping-activity-7199421691846942723-R5Kq/; and Bill Chappell, "What to know about the 'space weapon' the U.S. says Russia recently launched," NPR, May 30, 2024, https://www.npr.org/2024/05/30/nx-s1-4975741/what-to-know-russia-satellite-space-weapon-cosmos-2576.

4 Jim Shell (@jim-shell-4539438), "Russian satellite 'COSMOS 2576' (59773/2024-092A)- declared by US as a 'likely counterspace weapon' is on the move," LinkedIn, February 2025, https://www.linkedin.com/posts/jim-shell-4539438_russian-satellite-cosmos-2576-597732024-activity-7297837323893841920-a85_/.

5 *Russian Strategic Nuclear Forces* (blog), accessed March 5, 2025, https://russianforces.org/blog/.

6 "The Integrity Flash: Analysis of Developments in the Space Domain, Issue 116," Integrity ISR, March 9, 2025, https://isruniversity.com/wp-content/uploads/2025/03/116-9-Mar-2025-Integrity-Flash.pdf.

7 "COSMOS2581 82 83 LoweRes," Integrity ISR, YouTube video, March 7, 2025, https://www.youtube.com/watch?v=vhMDVW4eRUE.

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

9 Sandra Erwin, "Russian spy satellite reportedly continues suspicious maneuvers," *SpaceNews*, https://spacenews.com/russian-spy-satellite-reportedly-continues-suspicious-maneuvers/.

10 "Integrity Flash: Analysis of Developments in the Space Domain: Issue 115," Integrity ISR, February 24, 2025, https://isruniversity.com/wp-content/uploads/2025/02/115-24-Feb-2025-Integrity-Flash.pdf; "Satellite fleet: THOR 7," Space Norway, accessed April 15, 2024, https://spacenorway.com/infrastructure/satellite-fleet/thor-7/; and "Intelsat 10-02 at 359° E," Intelsat, accessed April 15, 2024, https://www.intelsat.com/fleetmaps/satellites/satellite_33/.

11 Kari A. Bingen, Kaitlyn Johnson, and Makena Young, *Space Threat Assessment 2023* (Washington, DC: CSIS, April 2023), https://www.csis.org/analysis/space-threat-assessment-2023.

12 "1+1 media's response to the enemy's attempts to jam Ukraine's satellite broadcasting," 1+1 Media, March 28, 2025, https://media.1plus1.ua/en/news/reakciia-11-media-na-sprobi-voroga-zaglusiti-suo putnikove-movlennia-ukrayini; "The Final Frontier Flash: Developments and Analysis in the Space Domain," Integrity ISR, April 7, 2024, https://isruniversity.com/wp-content/uploads/2024/04/94-7-Apr-2024-Final-Frontier-Flash.pdf; and "Sirius 4," NASA Space Science Data Coordinated Archive, accessed April 15, 2025, https://nssdc.gsfc.nasa.gov/nmc/spacecraft/display.action?id=2007-057A.

13 "Integrity Flash: Analysis of Developments in the Space Domain, Issue 118," Integrity ISR, April 8, 2025, https://isruniversity.com/2025/04/07/issue-118/.

14 Aamer Madhani and Zeke Miller, "Russia has obtained a 'troubling' emerging anti-satellite weapon, the White House says," AP News, February 15, 2024, https://apnews.com/article/russia-anti-satellite-weapon-threat-technology-2880f9c55122dcafe87188bc92dd6cde.

15 Unshin Lee Harpley, "DOD Official Confirms Russia Is Developing an 'Indiscriminate' Space Nuke,'" *Air and Space Forces Magazine*, May 2, 2024, https://www.airandspaceforces.com/dod-official-russia-indiscriminate-space-nuke/.

16 Jeff Foust, "U.S. Dismisses Space Weapons Treaty Proposal As 'Fundamentally Flawed,'" *SpaceNews*, September 11, 2014, https://spacenews.com/41842us-dismisses-space-weapons-treaty-proposeal-as-fundamentally-flawed/.

17 "The Nuclear Option: Deciphering Russia's New Space Threat," CSIS, May 3, 2024, https://www.csis.org/analysis/nuclear-option-deciphering-russias-new-space-threat.

18 "Cosmos-2553 – the first Neitron radar satellite," Russian strategic nuclear forces (blog), February 5, 2022, https://russianforces.org/blog/2022/02/cosmos-2553_-_the_first_neitro.shtml; and Pavel Podvig (@russianforces), "I think we can tell which satellite is responsible for the 'Russian nuclear something in space' scare. It's Cosmos-2553. Let's start with Mallory Stewart's statement earlier today at CSIS https://youtube.com/watch?v=dkDupSaxbOg… 1/," X, May 3, 2024, 6:28 p.m., https://x.com/russianforces/status/1786523272072331561.

19 W.J. Hennigan, "The Warning," *New York Times*, December 5, 2024, https://www.nytimes.com/interactive/2024/12/05/opinion/nuclear-weapons-space.html; General Stephen N. Whiting, Commander, U.S. Space Command, *Fiscal Year 2026 Priorities and Posture of United States Space Command*, Testimony before the U.S. Senate Armed Services Committee, 119th Cong., 1st sess. (March 26, 2025), https://www.armed-services.senate.gov/imo/media/doc/testimony_of_general_stephen_nwhiting.pdf; and Dr. John Plumb, U.S. Assistant Secretary of Defense for Space Policy, *FY25 Budget Request for National Security Space Programs*, Testimony before the U.S. House Armed Services Committee, 118th Cong., 2nd sess. (May 1, 2024), https://armedservices.house.gov/calendar/eventsingle.aspx?EventID=3536.

20 Theresa Hitchens, "Is Russia's Cosmos 2553 satellite a test for a future orbital nuclear weapon?," Breaking Defense, May 22, 2024, https://breakingdefense.com/2024/05/is-russias-cosmos-2553-satellite-a-test-for-a-future-orbital-nuclear-weapon/.

21 According to information provided to the report authors by LeoLabs on April 15, 2025.

22 Shaun Waterman, "Russian Jamming Is Wreaking Havoc on GPS in Eastern Europe. But Is It Hybrid Warfare?," *Air and Space Forces Magazine*, July 10, 2024, https://www.airandspaceforces.com/russian-gps-jamming-nato-ukraine/.

23 GPS Spoofing WorkGroup, *GPS Spoofing*.

24 Ryan Browne, "Russia jammed GPS during major NATO military exercise with US troops," CNN, November 14, 2018, https://www.cnn.com/2018/11/14/politics/russia-nato-jamming/index.html.

25 AFP, "Finland Developing Device to Counter Alleged Russian Satellite Jamming," The Defense Post, April 16, 2025, https://thedefensepost.com/2025/04/16/finland-russian-satellite-jamming/.

26 "Russia Expands GPS Signal Jamming to 15 Regions," *Moscow Times*, May 5, 2023, https://www.themoscowtimes.com/2023/05/05/russia-expands-gps-signal-jamming-to-15-regions-a81049.

27 "Attempts to Jam Suspilnes's Satellite Signal from Russian Territory Recorded," The Institute of Mass Information, August 25, 2024, https://imi.org.ua/en/news/attempts-to-jam-suspilne-s-satellite-signal-from-russian-territory-recorded-i47341.

28 "Satellite broadcasting of FREEDOM TV channel was attacked," FREEDOM, April 18, 2024, https://uatv.ua/en/satellite-broadcasting-of-freedom-tv-channel-was-attacked/; and "Cyber attack on TV channel BabyTV: Toddlers suddenly exposed to Russian propaganda," *NL Times*, April 6, 2024, https://nltimes.nl/2024/04/06/cyber-attack-tv-channel-babytv-toddlers-suddenly-exposed-russian-propaganda.

29 Emma Farge, "UN body condemns Russian satellite interference in Europe," Reuters, July 1, 2024, https://www.reuters.com/world/europe/un-body-condemns-russian-satellite-interference-europe-2024-07-01/.

30 Mabel Banfield-Nwachi, "Russia suspected of jamming GPS signal on aircraft carrying Grant Shapps," *The Guardian*, March 14, 2024, https://www.theguardian.com/politics/2024/mar/14/russia-suspected-of-jamming-gps-signal-on-aircraft-carrying-grant-shapps.

31 Maria Mamaeva," В РФ создали систему мониторинга «Калинка» для пеленгования сигналов Starlink," *Komsomolskaya Pravda*, December 14, 2024, https://www.kp.ru/online/news/6138843/.

32 Guy Faulconbridge and Dmitry Antonov, "Russia responds icily to U.S. hint on arms control talks with Moscow and Beijing," Reuters, March 20, 2024, https://www.reuters.com/world/russia-says-strategic-

talks-with-us-possible-only-part-broader-debate-2024-03-20/.

33 "Statement by the Representative of the Delegation of the Russian Federation at the Thematic Discussion on 'Outer Space (Disarmament Aspects)' in the First Committee of the 79th session of the UN General Assembly, New York, October 29, 2024," Ministry of Foreign Affairs of the Russian Federation, October 30, 2024, https://mid.ru/en/foreign_policy/news/1978174/.

OTHERS

1 Brett Tingley, "Iran launches 3 satellites on Simorgh rocket's 1st successful orbital launch," Space.com, January 29, 2024, https://www.space.com/iran-satellite-launches-middle-east-conflicts-january-2024; Nasser Karimi and Jon Gambrell, "Iran says it successfully launched a satellite in its program criticized by West over missile fears," Associated Press, September 14, 2024, https://apnews.com/article/iran-satellite-chamran-space-52022a743be4e3ffca5df9d30de7b04c; and Brett Tingley, "Iran launches military satellite, sending nation's largest-ever payload to orbit: reports," Space.com, December 6, 2024, https://www.space.com/space-exploration/launches-spacecraft/iran-launches-military-satellite-sending-nations-largest-ever-payload-to-orbit-reports.

2 "'Shorten The Timeline': Iran Touts Sending Heaviest Payload to Space as Nuclear Watchdogs Send Enrichment Warnings," Foundation for Defense of Democracies, *Flash Brief*, December 6, 2024, https://www.fdd.org/analysis/2024/12/06/shorten-the-timeline-iran-touts-sending-heaviest-payload-to-space-as-nuclear-watchdogs-send-enrichment-warnings/.

3 "Iran's Kowsar, Hodhod satellites successfully launched," Islamic Republic News Agency, November 5, 2024, https://en.irna.ir/news/85649902/Iran-s-Kowsar-Hodhod-satellites-successfully-launched.

4 Anatoly Zak, "Soyuz launches Russian-built satellite for Iran," Russian Space Web, last updated July 8, 2024, https://russianspaceweb.com/khayam.html.

5 Lily Hay Newman, "Notorious Iranian Hackers Have Been Targeting the Space Industry With a New Backdoor," *Wired*, August 28, 2024, https://www.wired.com/story/iran-peach-sandworm-tickler-backdoor/.

6 Tom Fakterman, Daniel Frank, and Jerome Tujague, "Curious Serpens' FalseFont Backdoor: Technical Analysis, Detection and Prevention," Unit42, March 21, 2024, https://unit42.paloaltonetworks.com/curious-serpens-falsefont-backdoor/; and Microsoft Threat Intelligence, "Peach Sandstorm deploys new custom Tickler malware in long-running intelligence gathering operations," Microsoft, August 28, 2024, https://www.microsoft.com/en-us/security/blog/2024/08/28/peach-sandstorm-deploys-new-custom-tickler-malware-in-long-running-intelligence-gathering-operations/.

7 Microsoft Threat Intelligence, "Peach Sandstorm password spray campaigns enable intelligence collection at high-value targets," Microsoft, September 14, 2023, https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-value-targets/.

8 Ofir Rozmann, Chen Evgi, and Jonathan Leathery, "When Cats Fly: Suspected Iranian Threat Actor UNC1549 Targets Israeli and Middle East Aerospace and Defense Sectors," Mandiant, February 27, 2024, https://cloud.google.com/blog/topics/threat-intelligence/suspected-iranian-unc1549-targets-israel-middle-east/.

9 Associated Press, "North Korean rocket carrying its 2nd spy satellite explodes shortly after launch," NBC News, May 27, 2024, https://www.nbcnews.com/news/world/north-korean-rocket-carrying-2nd-spy-satellite-explodes-shortly-launch-rcna154231.

10 "The Final Frontier Flash: Developments and Analysis in the Space Domain, Issue 100," Integrity ISR, June 30, 2024, https://isruniversity.com/wp-content/uploads/2025/02/100-30-Jun-2024-Final-Frontier-Flash.pdf.

11 Helen Regan, Gawon Bae, Brad Lendon, and Yumi Asada, "North Korea says it conducted new ICBM test, days ahead of US election," CNN, October 31, 2024, https://www.cnn.com/2024/10/30/asia/north-korea-icbm-test-intl-hnk/index.html; and Kim Tong-Hyung, "North Korea says it tested hypersonic intermediate range missile designed to strike remote Pacific targets," PBS, January 7, 2025, https://www.pbs.org/newshour/world/north-korea-says-it-tested-hypersonic-intermediate-range-missile-designed-to-strike-remote-pacific-targets.

12 Helen Regan, Alex Stambaugh, Gawon Bae, and Mariya Knight, "Blinken warns Russia is close to

sharing advanced satellite technology with North Korea," CNN, January 6, 2025, https://www.cnn.com/2025/01/06/asia/blinken-russia-satellite-technology-north-korea-intl-hnk/index.html.

13 "North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs," National Cyber Security Centre, July 25, 2024, https://www.ncsc.gov.uk/news/ncsc-partners-vigilant-dprk-sponsored-cyber-campaign.

14 Marco Galli et al., "An Offer You Can Refuse: UNC2970 Backdoor Deployment Using Trojanized PDF Reader," Mandiant, September 17, 2024, https://cloud.google.com/blog/topics/threat-intelligence/unc2970-backdoor-trojanized-pdf-reader.

15 "SpaDeX Mission," Indian Space Research Organization, December 21, 2024, https://www.isro.gov.in/mission_SpaDeX.html; and Geeta Pandey, "India successfully conducts historic space-docking test," BBC News, January 16, 2025, https://www.bbc.com/news/articles/c8j89k02py0o.

16 Abhinandan Mishra, "India may acquire advanced Russian radar system," *Sunday Guardian*, December 8, 2024, https://sundayguardianlive.com/news/india-may-acquire-advanced-russian-radar-system.

17 GPS Spoofing WorkGroup, *GPS Spoofing*.

18 Rudy Ruitenberg, "France plans low-orbit demonstrator that can target other satellites," *Defense News*, September 17, 2024, https://www.defensenews.com/global/europe/2024/09/17/france-plans-low-orbit-demonstrator-that-can-target-other-satellites/.

19 Mathieu Gitton (@mathieu-gitton), "France Intensifies Its Space Defense Strategy: New Challenges and Opportunities," LinkedIn, October 8, 2024, https://www.linkedin.com/pulse/france-intensifies-its-space-defense-strategy-new-mathieu-gitton-bxsce/.

GPS JAMMING AND SPOOFING

1 "UN agencies warn of satellite navigation jamming and spoofing," International Telecommunication Union, March 26, 2025, https://www.itu.int/hub/2025/03/un-agencies-warn-of-satellite-navigation-jamming-and-spoofing/.

2 Isabelle Khurshudyan and Alex Horton, "Russian jamming leaves some high-tech U.S. weapons ineffective in Ukraine," *Washington Post*, May 24, 2024, https://www.washingtonpost.com/world/2024/05/24/russia-jamming-us-weapons-ukraine/.

3 Linus Höller, "US, allies rush to refit their big guns with GPS protections," *Defense News*, March 13, 2025, https://www.defensenews.com/global/europe/2025/03/13/us-allies-rush-to-refit-their-big-guns-with-gps-protections/.

4 "Report a GPS Anomaly," Federal Aviation Administration, accessed March 19, 2025, https://www.faa.gov/air_traffic/nas/gps_reports.

5 Guy Buesnel and Mark Holbrow, "GNSS Threats, Attacks and Simulations," PNT Advisory Board, June 2017, https://www.gps.gov/governance/advisory/meetings/2017-06/buesnel.pdf.

6 Gleason Arliss, "What are the consequences of GPS interference?," Perfect Jammer, September 7, 2022, https://www.perfectjammer.com/what-are-consequences-interference.html.

7 Woodrow Bellamy III, "Are GPS Jamming Incidents a Growing Problem for Aviation?," *Avionics International*, January 31, 2017, https://www.aviationtoday.com/2017/01/31/are-gps-jamming-incidents-a-growing-problem-for-aviation/.

8 Matt Burgess, "When a tanker vanishes, all the evidence points to Russia," *Wired*, September 21, 2017, https://www.wired.com/story/black-sea-ship-hacking-russia/.

9 "2023 – The year of GPS jamming and spoofing," Resilient Navigation and Timing Foundation, January 27, 2024, https://rntfnd.org/2024/01/27/2023-the-year-of-gps-jamming-and-spoofing/.

10 GPS Spoofing WorkGroup, *GPS Spoofing*.

11 Ibid.

12 Hande Atay Alam et al., "Iran accuses Israel of killing Iranian military commanders and others in airstrike on consulate in Syria," CNN, April 1, 2024, https://edition.cnn.com/2024/04/01/middleeast/iran-syrian-consulate-attack-intl/index.html.

13 Laura Gozzi, "Ukraine war: Deepest Ukraine drone attack into Russian territory injures 12," BBC News, April 2, 2024, https://www.bbc.com/news/world-europe-68712158; Anna Chernova, Victoria Butenko,

and Sophie Tanno, “Ukraine claims major drone strike on Russian airfield, killing servicemen and destroying aircraft,” CNN, April 5, 2024, https://edition.cnn.com/2024/04/05/europe/ukraine-drone-strikes-rostov-region-russia-intl/index.html; and Olga Voitovych and Lauren Said-Moorhouse, “Russian oil refineries and military airfield targeted in drone attack, as thermal energy plants are damaged in Ukraine,” CNN, April 27, 2024, https://www.cnn.com/2024/04/27/europe/ukraine-russia-oil-refinery-drone-attack-intl/index.html.

14 Guy Faulconbridge and Lidia Kelly, “Ukraine attacks Moscow in one of largest ever drone strikes on Russian capital,” Reuters, August 21, 2024, https://www.reuters.com/world/europe/ukraine-launches-drone-attack-moscow-other-regions-russian-officials-say-2024-08-21/.

15 Maria Varenikova, “Ukraine Sends Volley of Drones at Russia, Hitting Oil Refinery,” *New York Times*, January 24, 2025, https://www.nytimes.com/2025/01/24/world/europe/ukraine-russia-oil-drone.html.

16 Pavel Polityuk and Alex Richardson, “Ukraine says it hit an offshore gas platform used by Russian forces,” Reuters, August 10, 2024, https://www.reuters.com/world/europe/ukraine-says-it-hit-an-offshore-gas-platform-used-by-russian-forces-2024-08-10/.

17 GPS Spoofing WorkGroup, GPS Spoofing.

18 Sribala Subramanian, “GPS Jamming in Myanmar,” *The Diplomat*, October 18, 2024, https://thediplomat.com/2024/10/gps-jamming-in-myanmar/.

19 Travis Turgeon, “Global GPS Jamming Hotspots: June 2024,” GNSS Jamming, July 1, 2024, https://www.gnssjamming.com/post/gps-jamming-report-june-2024; and John Feng, “North Korean Electronic Warfare Surges Under Kim: South,” *Newsweek*, October 4, 2024, https://www.newsweek.com/north-korea-gps-jamming-electronic-warfare-against-south-korea-surges-1963814.

20 GPS Spoofing WorkGroup, GPS Spoofing.

21 “ITU issues warning on interference with radio navigation satellite service,” International Telecommunication Union, August 23, 2022, https://www.itu.int/hub/2022/08/warning-harmful-interference-rnss/; and Stine Jacobsen and Anne Kauranen, “Estonia says Russia violates international rules with GPS interference,” Reuters, April 30, 2024, https://www.yahoo.com/news/estonia-says-russia-violates-international-083726782.html.

22 Kim Seung-yeon, “U.N. aviation agency voices grave concern over N. Korea’s GPS signal jamming,” Yonhap News Agency, June 24, 2024, https://en.yna.co.kr/view/AEN20240624008100315.

23 Agnes Helou, “Lebanon files complaint with UN over alleged Israeli GPS jamming,” *Breaking Defense*, July 17, 2024, https://breakingdefense.com/2024/07/lebanon-files-complaint-with-un-over-alleged-israeli-gps-jamming/.

24 Ionut Arghire, “Check Point Responds to Hacking Claims,” Security Week, April 1, 2025, https://www.securityweek.com/check-point-responds-to-hacking-claims/.

25 Yonatan Keller, “State actor or cybercrime? The story of IntelBroker, the most under-rated threat actor,” Zafran, April 25, 2024, https://www.zafran.io/resources/state-actor-or-cybercrime; and Waqas, “IntelBroker Claims Space-Eyes Breach, Targeting US National Security Data,” HackRead, April 16, 2024, https://hackread.com/intelbroker-space-eyes-breach-us-national-security-data/.

26 “European Repository of Cyber Incidents (EuRepoC),” German Institute for International and Security Affairs, accessed March 24, 2025, https://www.swp-berlin.org/en/swp/about-us/organization/swp-projects/european-repository-on-cyber-incidents-eurepoc.

27 Bill Toulas, “US Space Tech Giant Maxar Discloses Employee Data Breach,” BleepingComputer, November 18, 2024, https://www.bleepingcomputer.com/news/security/us-space-tech-giant-maxar-discloses-employee-data-breach.

28 Sandra Erwin, “Space Industry Group Warns of Escalating Cyber Threats, Outmatched Defenses,” *SpaceNews*, June 18, 2024, https://spacenews.com/space-industry-group-warns-of-escalating-cyber-threats-outmatched-defenses/; and Space ISAC Newsroom, accessed April 17, 2025, https://spaceisac.org/newsroom/#.

29 Clemence Poirer, “Hacking the Cosmos: Cyber operations against the space sector. A case study from the war in Ukraine,” Center for Security Studies, October 2024, https://css.ethz.ch/en/center/CSS-news/2024/10/hacking-the-cosmos-cyber-operations-against-the-space-sector-a-case-study-from-the-war-in-ukraine.html.

30 Austin Kaiser, "Satellite Hacking," Black Hills Information Security, October 3, 2024, https://www.blackhillsinfosec.com/satellite-hacking/.

31 Dale Arney et al., "In-Space Servicing, Assembly, and Manufacturing (ISAM) State of Play - 2024 Edition," NASA Technical Reports Server, October 31, 2024, https://ntrs.nasa.gov/citations/20240012414.

32 "Space Symposium 40: Whiting stressed U.S. must prepare for conflict to ensure peace," U.S. Space Command, April 8, 2025, https://www.spacecom.mil/Newsroom/News/Article-Display/Article/4149678/space-symposium-40-whiting-stressed-us-must-prepare-for-conflict-to-ensure-peace/; and Achala Dennison, "Why Orbital Maneuvering Is Top Of Mind At U.S. Space Command," Space Systems CyberSecurity, October 7, 2024, https://spacesecurity.wse.jhu.edu/2024/10/07/https-aviationweek-com-space-launch-vehicles-propulsion-why-orbital-maneuvering-top-mind-us-space-command/.

33 "Geosynchronous Space Situational Awareness Program," United States Space Force, last updated October 2020, https://www.spaceforce.mil/About-Us/Fact-Sheets/Article/2197772/geosynchronous-space-situational-awareness-program/.

34 Garrett Reim, "SSC Researching Constellation Of Next-Generation GEO Satellite Scouts," Aviation Week Network, March 11, 2024, https://aviationweek.com/space/ssc-researching-constellation-next-generation-geo-satellite-scouts.

35 Sandra Erwin, "True Anomaly Achieves Milestone with Jackal Satellite Deployment," *SpaceNews*, December 26, 2024, https://spacenews.com/true-anomaly-achieves-milestone-with-jackal-satelelite-deployment/; and "Mission X Continues: Announcing Successful Launch and Control of Jackal," True Anomaly, December 21, 2024, https://www.trueanomaly.space/newsroom/mission-x-continues.

36 "Identification and Characterisation of Space Objects Through Non-Earth Imaging," HEO, https://www.heospace.com/white-papers/identification-and-characterisation-of-space-objects-through-non-earth-imaging.

37 Tom Temin, "Air Force Research Lab Creates a New Approach to Situational Awareness in Space," Federal News Network, January 26, 2024, https://federalnewsnetwork.com/air-force/2024/01/air-force-research-lab-creates-a-new-approach-to-situational-awareness-in-space/.

38 Debra Werner, "French Armament Agency Responds to Space Threats," SpaceNews, September 17, 2024, https://spacenews.com/french-armament-agency-responds-to-space-threats/; Rudy Ruitenberg, "France Plans Low-Orbit Demonstrator That Can Target Other Satellites," *Defense News*, September 17, 2024, https://www.defensenews.com/global/europe/2024/09/17/france-plans-low-orbit-demonstrator-that-can-target-other-satellites/; and Nicolas Cailleaud, "Espace: Tout Savoir Sur Yoda, CET Engin de Guerre Protecteur de Satellites," CNEWS, April 29, 2021, https://www.cnews.fr/science/2021-04-29/espace-tout-savoir-sur-yoda-cet-engin-de-guerre-protecteur-de-satellites-1076052.

39 "The Iron Dome for America," The White House, January 27, 2025, https://www.whitehouse.gov/presidential-actions/2025/01/the-iron-dome-for-america/.

40 "Implementing Competitive Endurance: Space Intelligence," CSIS, October 10, 2023, https://www.csis.org/analysis/implementing-competitive-endurance-space-intelligence.

41 Darren McKnight et al., "Rocket Body Tumbling Assessment Through Radar, Optical Telescope, and Imaging," 75th International Astronautical Congress (IAC), October 14–18, 2024, https://ccd.aiub.unibe.ch/publist/data/2024/artproc/SF_IAC2024.pdf.

42 Jim Garamone, "Iran Shoots Down U.S. Global Hawk Operating in International Airspace," DOD News, June 20, 2019, https://www.defense.gov/News/News-Stories/article/article/1882497/iran-shoots-down-us-global-hawk-operating-in-international-airspace/; U.S. Air Forces Europe - Air Forces Africa,"Russian aircraft collides into US unmanned system in international waters," U.S. European Command, March 14, 2023, https://www.eucom.mil/pressrelease/42314/russian-aircraft-collides-into-us-unmanned-system-in-international-waters; Jim Garamone, "Defense Leaders See Increase in Risky Chinese Intercepts," DOD News, June 8, 2023, https://www.defense.gov/News/News-Stories/Article/Article/3421766/defense-leaders-see-increase-in-risky-chinese-intercepts/; and John Feng, "U.S. and China Spar Over Military Aircraft Intercept Over South China Sea," *Newsweek*, January 2, 2023, https://www.newsweek.com/us-china-military-aircraft-us-air-force-peoples-liberation-army-navy-south-china-sea-1770666.

43 Per discussions in March 2024 with an individual close to TraCSS implementation efforts.

44 Jim Shell (@jim-shell-4539438), "OUCH! Russia slams the US over the lack of cataloging debris asso-

ciated with recent US space object breakups!" LinkedIn, February 2025, https://www.linkedin.com/posts/jim-shell-4539438_ouch-russia-slams-the-us-over-the-lack-activity-7298535252027748354-yeAD.

45 The eight incidents selected were based on information discoverable from SSA experts and companies on social media, cited below.

46 U.S. Space Command, "Break-up of Russian-owned space object," press release, June 27, 2024, https://www.spacecom.mil/Newsroom/News/Article-Display/Article/3819238/press-release-break-up-of-russian-owned-space-object/; and Reuters, "Astronauts take cover as defunct Russian satellite splits into nearly 200 pieces," The Guardian, June 27, 2024, https://www.theguardian.com/science/article/2024/jun/27/russian-satellite-debris-international-space-station.

47 LeoLabs (@LeoLabs_Space), "We're actively monitoring and analyzing the breakup event in #LEO involving a Chinese rocket body, CZ-6A. Our radar data indicates this event occurred on 6 August at ~20:10 UTC at ~810 km. It resulted in at least 700 debris fragments and potentially more than 900," X, August 8, 2024, 6:28 p.m. ET, https://x.com/LeoLabs_Space/status/1821674976245670386.

48 Ibid.

49 Jim Shell (@jim-shell-4539438), "YASDE! (Yet Another Space Debris Event)," LinkedIn, September 2024, https://www.linkedin.com/posts/jim-shell-4539438_spacesustainability-spacedebris-spacedopmainnormsofbehavior-activity-7237837766460342272-ySgV.

50 S4S_SDA, "S4S has confirmed the breakup of Intelsat 33E (#41748, 2016-053B) ~0430 UTC. Currently tracking around 20 associated pieces - analysis ongoing," X, October 19, 2024, 9:56 p.m. ET, https://x.com/S4S_SDA/status/1847819183272472884.

51 Jason Rainbow, "ExoAnalytic observes 500 pieces of debris from Intelsat 33e breakup," *SpaceNews*, October 28, 2024, https://spacenews.com/exoanalytic-observes-500-pieces-of-debris-from-intelsat-33e-breakup/.

52 Jeff Foust, "Retired military weather satellite breaks up," *SpaceNews*, December 20, 2024, https://spacenews.com/retired-military-weather-satellite-breaks-up.

53 Slingshot Aerospace, "Slingshot Orbital Alert," X, December 19, 2024, 4:15 p.m. ET, https://x.com/sling_shot_aero/status/1869853991296741726.

54 Jim Shell (@jim-shell-4539438), "YASDE! (Yet Another Space Debris Event)," LinkedIn, February 2025, https://www.linkedin.com/posts/jim-shell-4539438_longtermsustainmentofspace-spacedomainawareness-activity-7291070798121836545-b8WA.

55 Ibid.

56 Jim Shell (@jim-shell-4539438), "YASDE! (Yet Another Space Debris Event)," LinkedIn, October 2024, https://www.linkedin.com/posts/jim-shell-4539438_spacedebris-activity-7250519127235182592-miAS.

57 "Fregat RB/Cluster 2," NASA, March 26, 2025, https://nssdc.gsfc.nasa.gov/nmc/spacecraft/display.action?id=2000-015A; and Jim Shell (@jim-shell-4539438), "A LOT of #SpaceDebris with LITTLE awareness," LinkedIn, September 2024, https://www.linkedin.com/posts/jim-shell-4539438_spacedebris-spacesustainability-activity-7241669796587565056-_wYm.

58 Jim Shell, "A LOT of #SpaceDebris with LITTLE awareness," LinkedIn, September 2024.

59 "NATO explores ways to better protect commercial partners in space," NATO, October 4, 2024, https://www.nato.int/cps/en/natohq/news_229236.htm.

60 "Russia warns United States: use of SpaceX for spying makes its satellites a target," Reuters, March 20, 2024, https://www.reuters.com/world/russia-warns-united-states-use-spacex-spying-makes-its-satellites-target-2024-03-20/.

61 Clyde Laheyne, "Forging the space armory," Dark, January 28, 2025, https://www.dark-space.co/mission-forging-the-space-armory.

62 Aria Alamalhodaei, "Dark is building a rocket-powered boxing glove to push debris out of orbit," TechCrunch, April 17, 2024, https://techcrunch.com/2024/04/17/dark-space-is-building-a-rocket-powered-boxing-glove-to-push-debris-out-of-orbit/.

63 Tereza Pultarova, "Astroscale, BAE Systems Team On ISAM Demo by 2030," Payload, March 5, 2025,

https://payloadspace.com/astroscale-bae-systems-team-on-isam-demo-by-2030/.

64 "RemoveDEBRIS," Airbus, accessed April 17, 2025, https://www.airbus.com/en/products-services/space/earth-observation/removedebris.

WHAT TO WATCH

1 "White Paper on Competitive Endurance: A Proposed Theory of Success for the U.S. Space Force," United States Space Force, January 11, 2024, https://www.spaceforce.mil/Portals/2/Documents/White_Paper_Summary_of_Competitive_Endurance.pdf.

2 "Tenets of Responsible Behavior in Space," Secretary of Defense, July 7, 2021, https://www.spacecom.mil/Newsroom/Publications/Pub-Display/Article/3318236/tenets-of-responsible-behavior-in-space/.

3 "USSPACECOM Releases Specific Behaviors," U.S. Space Command, March 3, 2023, https://www.spacecom.mil/Newsroom/News/Article-Display/Article/3318606/usspacecom-releases-specific-behaviors/.

4 Sandra Erwin, "U.S. declares ban on anti-satellite missile tests, calls for other nations to join," *SpaceNews*, April 18, 2022, https://spacenews.com/u-s-declares-ban-on-anti-satellite-missile-tests-calls-for-other-nations-to-join/; and Jeff Foust, "United Nations General Assembly approves ASAT test ban resolution," *SpaceNews*, December 13, 2022, https://spacenews.com/united-nations-general-assembly-approves-asat-test-ban-resolution/.

5 Eric Lipton, "Departing Air Force Secretary Will Leave Space Weaponry as a Legacy," *New York Times*, December 29, 2024, https://www.nytimes.com/2024/12/29/us/politics/frank-kendall-air-force.html; and Theresa Hitchens, "'Space fires' to enable 'space superiority' are top SPACECOM priorities for FY27," *Breaking Defense*, August 6, 2024, https://breakingdefense.com/2024/08/space-fires-to-enable-space-superiority-are-top-spacecom-priorities-for-fy27/.

6 "Rules of war (in a nutshell)," International Committee of the Red Cross, August 22, 2014, https://www.icrc.org/en/document/rules-war-nutshell.

7 "Agreement Between the Government of The United States of America and the Government of The Union of Soviet Socialist Republics on the Prevention of Incidents On and Over the High Seas," U.S. Department of State, entered into force May 25, 1972, https://2009-2017.state.gov/t/isn/4791.htm.

8 Space and Missile Systems Center Public Affairs, "Counter Communications System Block 10.2 achieves IOC, ready for the warfighter," United States Space Force, March 13, 2020, https://www.spaceforce.mil/News/Article/2113447/counter-communications-system-block-102-achieves-ioc-ready-for-the-warfighter/; and "STARCOM tests RMT system for Space Rapid Capabilities Office," Space Training and Readiness Command (STARCOM), April 18, 2024, https://www.starcom.spaceforce.mil/News/Article-Display/Article/3747374/starcom-tests-rmt-system-for-space-rapid-capabilities-office/.

9 Theresa Hitchens, "Space Force's FY24 budget includes 'offensive' options for space. What does that mean?" *Breaking Defense*, March 13, 2023, https://breakingdefense.com/2023/03/space-forces-fy24-budget-includes-offensive-options-for-space-what-does-that-mean/; and "Remarks by Deputy Secretary of Defense Kathleen H. Hicks at the U.S. Space Command (USSPACECOM) Change of Command Ceremony (As Delivered)," U.S. Department of Defense, January 10, 2024, https://www.defense.gov/News/Speeches/Speech/Article/3641746/remarks-by-deputy-secretary-of-defense-kathleen-h-hicks-at-the-us-space-command/.

10 Britianie Teston, "Innovative Testing and Skilled Personnel Drive Space RCO's Newest Success," Kirtland Air Force Base, October 7, 2024, https://www.kirtland.af.mil/News/Article-Display/Article/3928036/innovative-testing-and-skilled-personnel-drive-space-rcos-newest-success/; and Christopher Stone, "Space-to-ground capabilities are the answer to deterring invasion of Taiwan," *Space Review*, January 30, 2023, https://www.thespacereview.com/article/4522/1.

11 European Defense Fund factsheet, "Bodyguard," European Commission, May 16, 2024, https://defence-industry-space.ec.europa.eu/document/download/dfcec3d7-df67-4fc4-a7ea-0e5362ce204c_en?filename=EDF-2023-RA-SPACE-PSA%20BODYGUARD.pdf.

12 Angela Webb, "Joint Effort Made Satellite Success Possible," U.S. Strategic Command, February 25, 2008, https://www.stratcom.mil/Media/News/News-Article-View/Article/983539/joint-effort-made-satellite-success-possible/.

13 Jeff Foust, "Majority of tracked Russian ASAT debris has deorbited," *SpaceNews*, September 29, 2022,

https://spacenews.com/majority-of-tracked-russian-asat-debris-has-deorbited/; and Space-Track Catalogue, accessed on March 24, 2025, https://www.space-track.org/#catalog.

14 Space-Track.org, Accessed on April 2, 2025.

15 Andrew Jones, "China's megaconstellation launches could litter orbit for more than a century, analysts warn," *SpaceNews*, April 7, 2025, https://spacenews.com/chinas-megaconstellation-launches-could-litter-orbit-for-more-than-a-century-analysts-warn/.

16 While this development would mark the first reported space-based nuclear ASAT capability believed to target pLEO constellations, high-altitude nuclear detonations (HANDs) in space are not new. In fact, any actor with a nuclear warhead and medium-range ballistic missile possesses such a latent capability. Both the United States and Soviet Union conducted HAND tests in the 1950s and 1960s, including the 1962 U.S. Starfish Prime test notable for the damage and destruction it caused to orbiting satellites at the time through prompt and delayed, or accumulating, radiation. An orbiting nuclear ASAT would present a challenging warning problem and—depending on the altitude, placement, and magnitude of the detonation—would create catastrophic devastation in low Earth orbit for months to years.

17 Kari A. Bingen, Kaitlyn Johnson, and Makena Young, *Space Threat Assessment 2023* (Washington, DC: CSIS, April 2023), https://www.csis.org/analysis/space-threat-assessment-2023.

18 "Russia warns United States: use of SpaceX for spying makes its satellites a target," Reuters, March 20, 2024, https://www.reuters.com/world/russia-warns-united-states-use-spacex-spying-makes-its-satellites-target-2024-03-20/; and "Russia warns West: We can target your commercial satellites," Reuters, October 27, 2022, https://www.reuters.com/world/russia-says-wests-commercial-satellites-could-be-targets-2022-10-27/.

19 General Stephen N. Whiting, Commander, U.S. Space Command, *Fiscal Year 2026 Priorities and Posture of United States Space Command*, Testimony before the U.S. Senate Armed Services Committee, 119th Cong., 1st sess. (March 26, 2025), https://www.armed-services.senate.gov/imo/media/doc/testimony_of_general_stephen_nwhiting.pdf.

20 "The Iron Dome for America," The White House, January 27, 2025, https://www.whitehouse.gov/presidential-actions/2025/01/the-iron-dome-for-america/.

21 D. K. Barton et al, "Report of the American Physical Society Study Group on Boost-Phase Intercept Systems for National Missile Defense: Scientific and Technical Issues," Rev. Mod. Phys. 76, S1 (2004), https://journals.aps.org/rmp/abstract/10.1103/RevModPhys.76.S1.

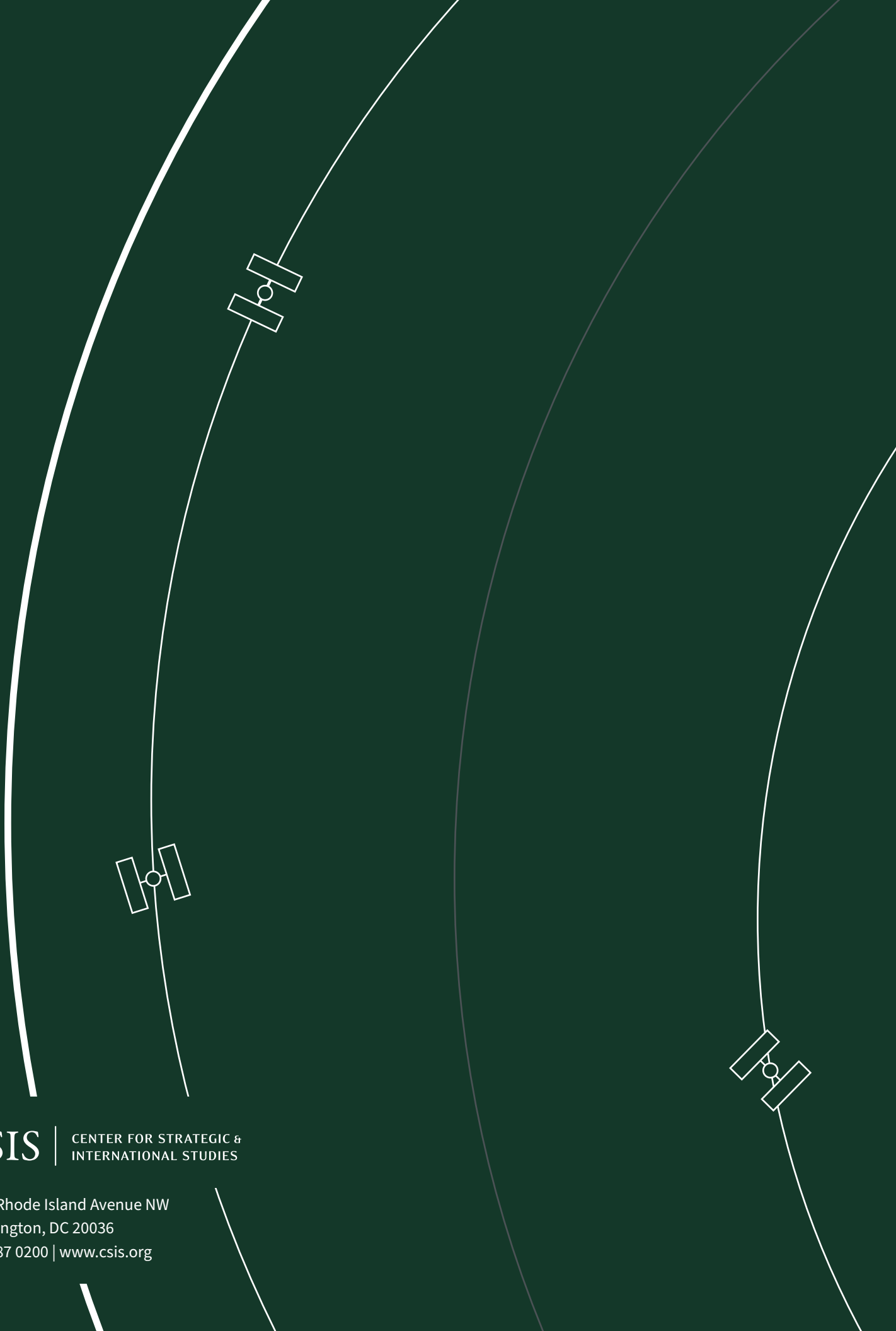
22 Jon Jackson, "Russia Rebukes Donald Trump's Plan for American Iron Dome," *Newsweek*, January 31, 2025, https://www.newsweek.com/russia-trump-iron-dome-2024329.

23 "Space Force announces new mission statement," Secretary of the Air Force Public Affairs, September 6, 2023, https://www.spaceforce.mil/News/Article-Display/Article/3517324/space-force-announces-new-mission-statement/.

CONCLUSION

1 Greg Hadley, "'Whatever it Takes': Saltzman Says 'Space Superiority' Is USSF's Mission," *Air and Space Forces Magazine*, March 3, 2025, https://www.airandspaceforces.com/saltzman-space-force-destruction-offensive-space/.

2 "Space Symposium 40: Whiting stressed U.S. must prepare for conflict to ensure peace."



CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

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