Recorded Future®

The Convergence of Space and Cyber

Joseph Rooke
January 2025

Executive Summary

Cyber-attacks will play a critical role in determining who dominates the second space race. As this new race accelerates, so too will the frequency and sophistication of cyber-attacks targeting organisations operating in the space domain. Understanding this evolving threat landscape is essential to preparing for the challenges ahead.

The first space race was a contest for supremacy between the United States and the Soviet Union. Following the Soviet Union's collapse, the United States emerged as the dominant space power. Fast forward to the 2020s and a new race has begun. China has entered the arena with its Taikonauts, Bedoui-3 satellites and Chang'e space missions. Russia appears to be partnering with China to challenge the United States and its allies. Additionally, countries like India, Israel, and the UAE are making significant strides to establish themselves as space powers.

The stakes are high. Space offers unprecedented opportunities to harness resources and expand humanity's presence beyond Earth. Whoever dominates space will, ultimately, dominate Earth. This has led to a rapid militarisation of space and an influx of private companies eager to claim their share of this new frontier, as we will explore later in this paper. Alongside these developments, cyber-attacks targeting space infrastructure, organisations, and supply chains have intensified.

This white paper aims to provide a comprehensive understanding of the unfolding 21st-century space race. More importantly, it highlights how vulnerable space-related organisations, industries, and supply chains are to cyber-attacks as competition accelerates.

Key Findings:

- The race for dominance in Earth's orbit is well underway. Future phases will focus on returning to the Moon, mining asteroids, and exploring other planets.
- Leading nations like the United States, China, Russia, the European Union, and India are investing heavily in space missions and capabilities. Meanwhile, emerging space powers such as Israel, South Korea, Japan, and the United Arab Emirates are rapidly advancing their efforts.
- Over the past five years, numerous nations have announced the creation of dedicated Space Forces and Commands. Notably, cyber capabilities are increasingly being integrated alongside space assets, offering both defensive and offensive options.
- Since the mid-2010s, there has been a noticeable increase in cyber-attacks targeting space operations, including signal jamming, destructive attacks, and supply chain compromises.
- Offensive and defensive cyber operations will be pivotal in determining the outcomes of the second space race.

Background

Space-related developments will influence every industry. Our businesses depend on navigation systems like GPS for logistics and operations. Financial services firms have substantial investments in the space sector. Mining companies will face new dynamics as asteroid mining becomes a reality. The energy sector could be transformed if helium-3, a potential fusion energy source, is successfully transported from the Moon to Earth. Telecommunications systems are increasingly reliant on satellite networks to provide seamless global connectivity. Meanwhile, military operations heavily utilise assets in space to conduct missions. The list of space-driven impacts is extensive and growing.

Much of the current and future space capabilities are and will be controlled from ground stations. Effectively, Earth will direct space operations, and for the time being Earth will continue to manufacture technologies used in space operations. Ground stations and factories are vulnerable to cyber-attacks and should be our main focus in the short term. Cyber attacks targeting space-related organisations and their supply chains are becoming increasingly common. As we will also explore, nations such as the United States and China are combining space and cyber capabilities for this very reason.

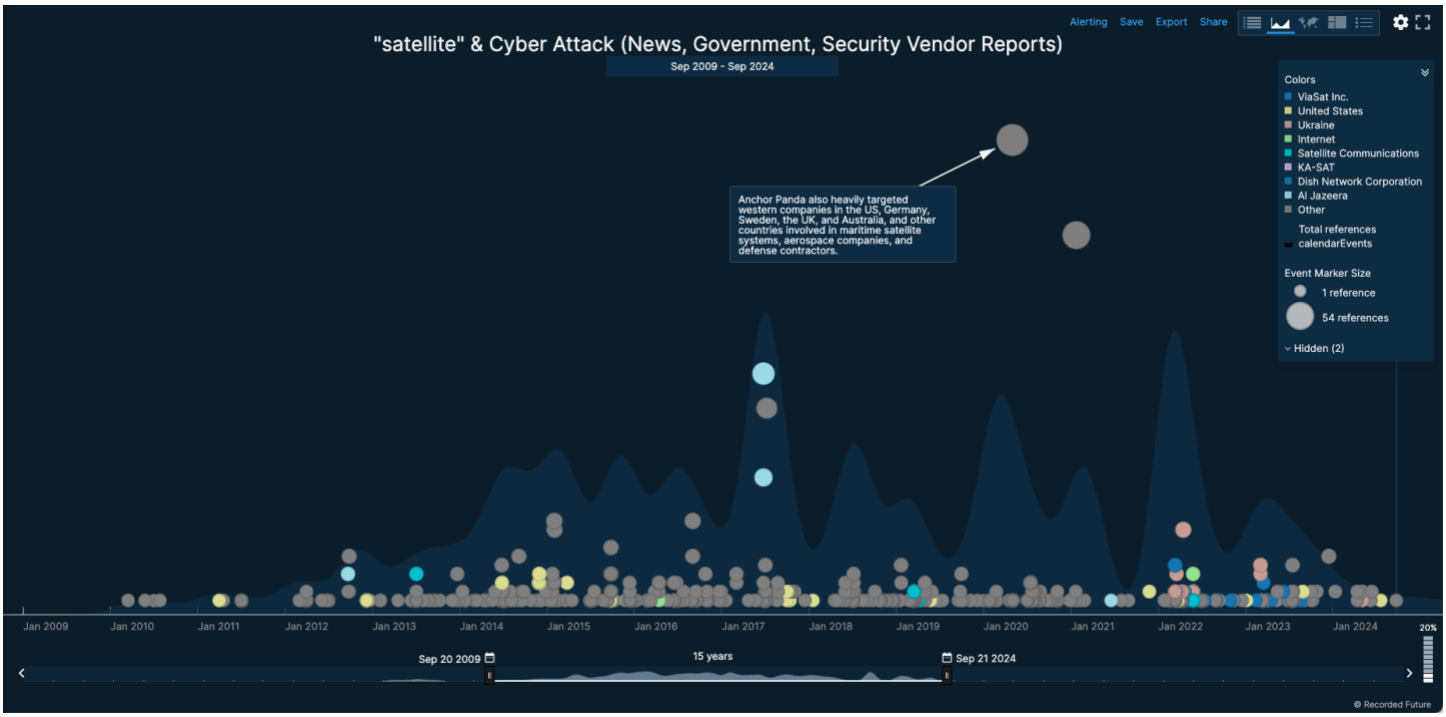

Figure 1: *Timeline from 2019 to 2024 showing references on News, Government Security Vendor Sources of cyber attacks related to "satellite". The trend shows an uptick in recent years.*

This paper examines the evolving space race, the major powers competing for dominance, the role of cyber-attacks, and the steps we must take to prepare for a growing number of space-related cyber threats. Special attention will be given to the intensifying competition between the United States and China, both of which possess advanced cyber capabilities and a clear ambition to dominate space.

The Stages of the Race

Before we explore how cyber attacks are impacting space-related activities, we need to understand the current 21st century space race that is unfolding.

Earth's orbit is becoming increasingly congested with a growing number of satellites being launched by an ever-growing list of countries. The Moon has huge potential to act as a launch pad for space exploration and is rich in minerals, there are missions planned to colonise the moon in the 2020s and 2030s. Meanwhile, asteroids, containing vast reserves of minerals, are poised to become targets for resource extraction. The successful mining of these celestial bodies could generate immeasurable wealth for countries and corporations alike. Finally, planetary exploration is advancing with the long-term goal of identifying and establishing permanent human settlements beyond Earth.

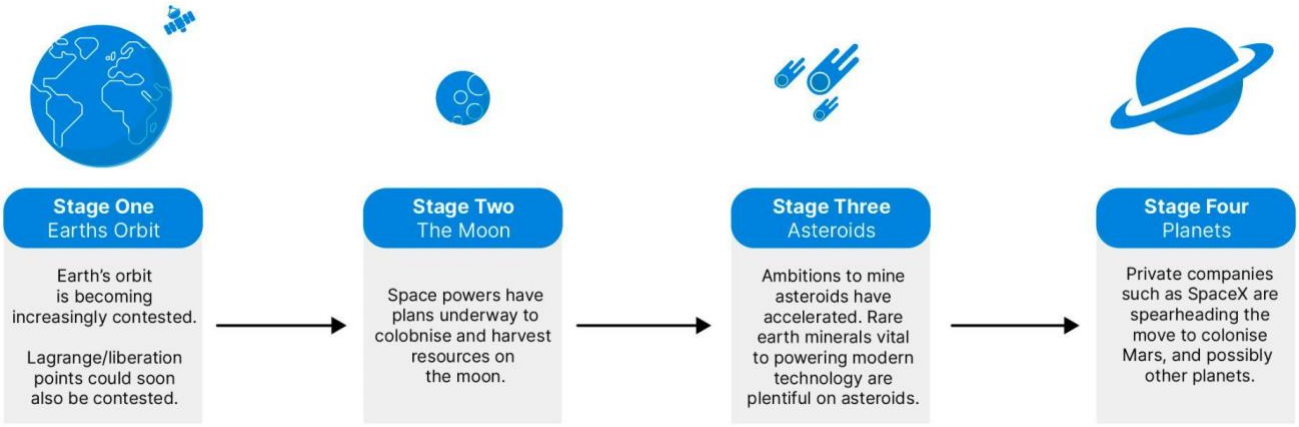

Figure 2: *Stages of the space race that are unfolding.*

Satellites

Low Earth Orbit (LEO), Medium Earth Orbit (MEO), and High Earth Orbit (HEO) serve as strategic positions for various types of satellites that support essential functions such as communication, navigation, military operations, scientific research, and national security.

Low Earth Orbit (LEO): 180 to 2,000 km above Earth
Medium Earth Orbit (MEO): 2,000 to 35,786 km above Earth
High Earth Orbit (HEO): Above 35,786 km (includes Geostationary Orbit, GEO)

LEO is typically used for satellites that provide high-speed internet or phone services as they are closer to Earth and therefore can transmit that data much quicker and with a lower latency. Earth observation satellites are also often located in LEO and used for weather forecasting, disaster response, environmental monitoring and military reconnaissance. Scientific research assets such as the International Space Station (ISS) operate here also, where they are better placed to study Earth.

MEO is where we can find navigation satellite systems such as Global Positioning System (GPS), GLONASS, Galileo and Beidou. They are critical for both civilian and military applications as they provide critical positioning, navigation, and timing (PNT) services. If these satellites were to fail, the global economic consequences would be catastrophic. Some communications satellites also operate in MEO, and tend to have a broader coverage, though with higher latency.

HEO often hold geostationary satellites, where they can remain fixed relative to a point on the Earth's surface. Weather satellites and military surveillance assets often operate in HEO. Furthermore, this is where militaries often choose to place missile early warning systems, giving nations strategic and defensive capabilities.

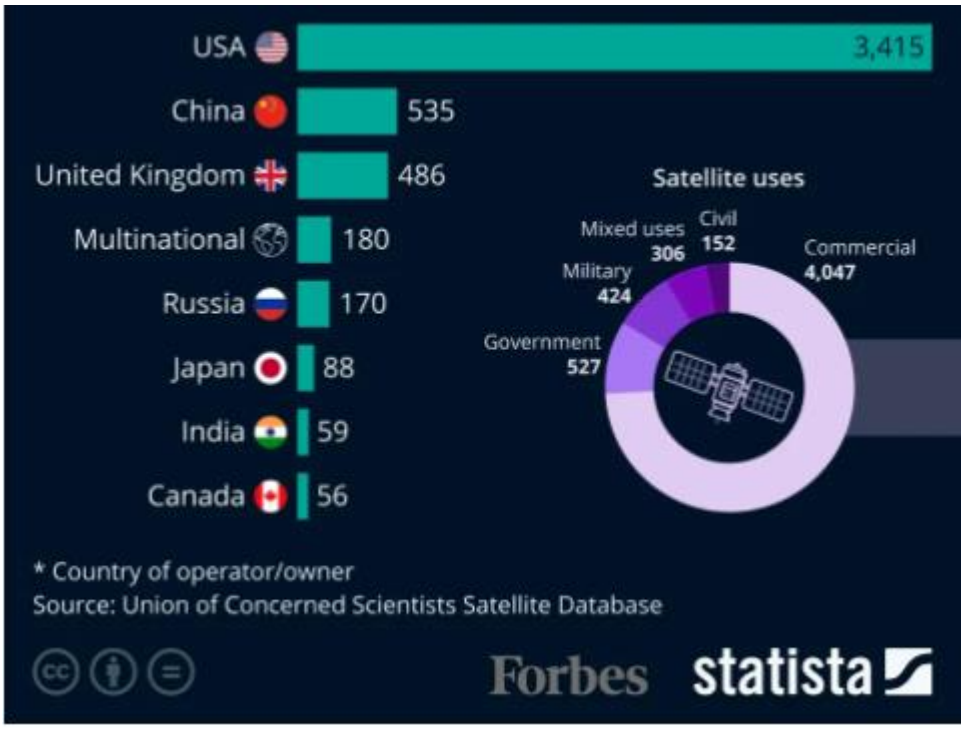

Figure 3: *Infographic taken from Forbes website showing the satellites orbiting Earth by country as of May 2022.*

The United States has a clear advantage in the number of satellites in space, however, the landscape is evolving rapidly with advancements in technology and the expansion of satellite constellations. China is expanding its Beidou Navigation Satellite System (BDS) programme. The Beidou system is designed to provide global navigation services and reduce Beijing's reliance on the US-owned GPS. China has ambitious plans to enhance its communication infrastructure, both for terrestrial and space-based networks. It is also deploying more satellites for Earth observation purposes. There are also other countries that are capable of launching and running navigation satellites.

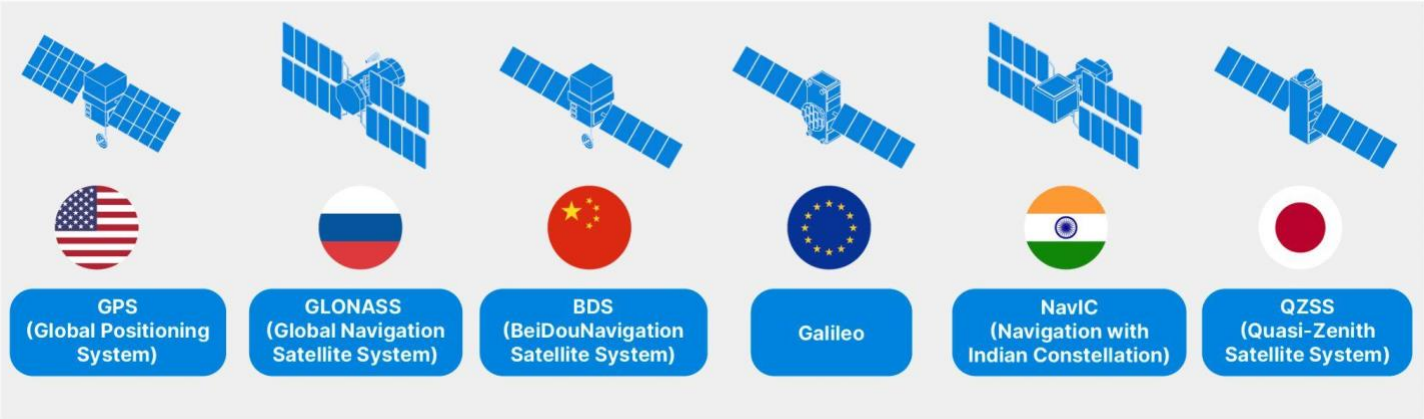

Figure 4: *Summary of key navigation satellites currently in Earth's orbit.*

There is a space beyond HEO which we should briefly mention: Lagrange points. There are five specific positions in space where the gravitational forces of two large celestial bodies, like the Earth and the Sun, or the Earth and the Moon, balance the centripetal force felt by a smaller object. This balance allows an object to remain in a stable or semi-stable position relative to the two larger bodies. To simplify this concept, think of Lagrange points as parking lots in space.

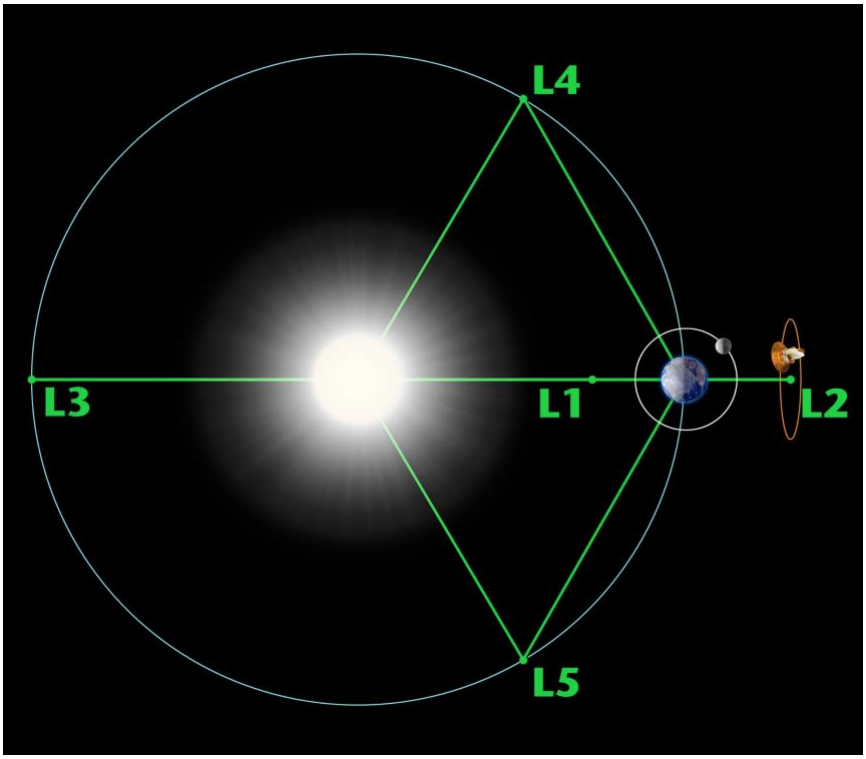

Figure 5: *Image of Lagrange points taken from NASA website.*

Lagrange points are important because they offer unique gravitationally balanced positions in space where spacecraft, satellites, and other objects can "park" with minimal energy requirements. These points therefore provide strategic advantages. They could serve as continuous observation points, communication relay points, space habitats or staging areas for missions travelling to other planets.

Cyber attacks to date have commonly focused on the targeting of assets such as satellites, operating in Earth's LEO. This highlights the growing convergence of space operations and cyber operations and will be explored in later sections of the white paper.

The Moon

Between 1969 and 1972 there were a total of 6 crewed landings on the Moon, all conducted by the United States Apollo programme. There were no future soft landings on the Moon, until 2013, when China successfully landed Chang'e 3. All landings took place on the near side of the Moon, until 2019 when China's Chang'e 4 made the first landing on the far side of the Moon, there was a reason for the Chang'e missions.

The Moon contains valuable resources:

Water Ice: NASA's SOFIA mission confirmed water exists on the Moon. Permanently shadowed craters at the lunar poles could hold water ice that would be critical for supporting human life and can be split into hydrogen and oxygen which in turn could be used for rocket fuel, enabling deeper space exploration.

Helium-3: This isotope has potential as a fuel for future nuclear fusion reactors, offering a cleaner and more efficient energy source. If humans can find a way to harvest and transport Helium-3 on the Moon, this could power Earth's energy needs for thousands of years. NASA estimates there could be a million tonnes of Helium-3 on the Moon.

Minerals & Rare Earth Elements: The Moon's surface is believed to hold valuable minerals such as platinum and other rare earth elements, essential for various technologies. According to Boeing, the Moon contains scandium, yttrium and the 15 lanthanides, also vital to powering future electronics. The lunar soil contains titanium and iron. They could be used in construction and manufacturing processes for building infrastructure on the Moon.

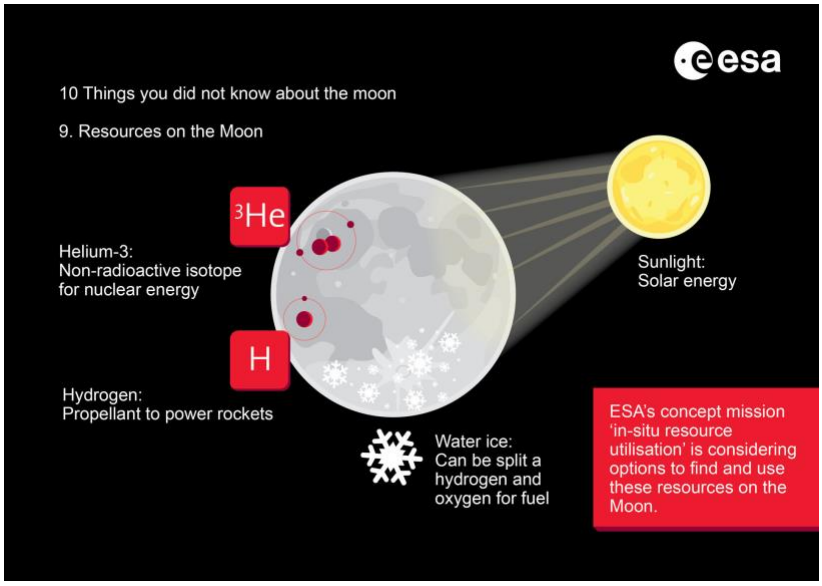

Figure 6: *Infographic taken from The European Space Agency (ESA) website highlighting some of the resources on the Moon and how the ESA's concept mission is "considering options to find and use these resources".*

Countries such as the United States and China are now racing to reach the Moon and establish a presence. There are also a large number of private companies developing plans and technology to mine the Moon.

Figure 7: *Infographic taken from Orbital Today showing a ranking of Moon Mining Companies in 2023.*

The U.S.-led Artemis programme, run by NASA, aims to explore lunar resources and plans to establish a sustainable human presence. NASA also plans on utilising resources mined on the Moon for deeper space missions. NASA aims to launch its first crewed mission around the Moon in 2025, also referred to as Artemis II. The following mission, Artemis III, planned for 2026, aims to land the first astronauts near the lunar South Pole.

China's Chang'e program includes lunar missions focusing on resource exploration. China's long-term goals involve mining lunar resources to support its lunar base and space exploration objectives. In 2024 Chang'e 6 returned samples from the far side of the Moon, making it a true rival to the ambitions of the United States.

India's ISRO's Chandrayaan missions are actively investigating lunar resources, particularly water ice, to support future exploration and potential in-situ resource utilisation. In 2024, Chandrayaan-3 successfully landed on the Moon.

Russia is planning lunar missions such as Luna-25, Luna-26, and Luna-27 to study and potentially exploit lunar resources as part of its broader space exploration strategy which involves sending cosmonauts to the Moon in the next decade.

There are multiple challenges but also many benefits to be gained by returning to the Moon and establishing a presence in the form of colonies. The lack of space regulation, combined with the scramble to secure resources on the Moon is likely to create tensions between competing nations, in particular between the United States and China.

Cyberattacks related to gathering information on other nations' Moon operations and technology are likely to accelerate. The section later in this report highlights how already companies involved in enabling future Moon exploration have been victims of cyberattacks.

Asteroids

Similar to the Moon, Asteroids are rich in metals such as platinum, gold, nickel, and iron. These metals are valuable for electronics and potential space infrastructure.

If we were to value asteroids based on the current prices of metals on Earth, they would be in the quintillions of USD. This makes the idea of launching missions to mine them attractive to many companies as profits could reach trillions of dollars from just a few missions.

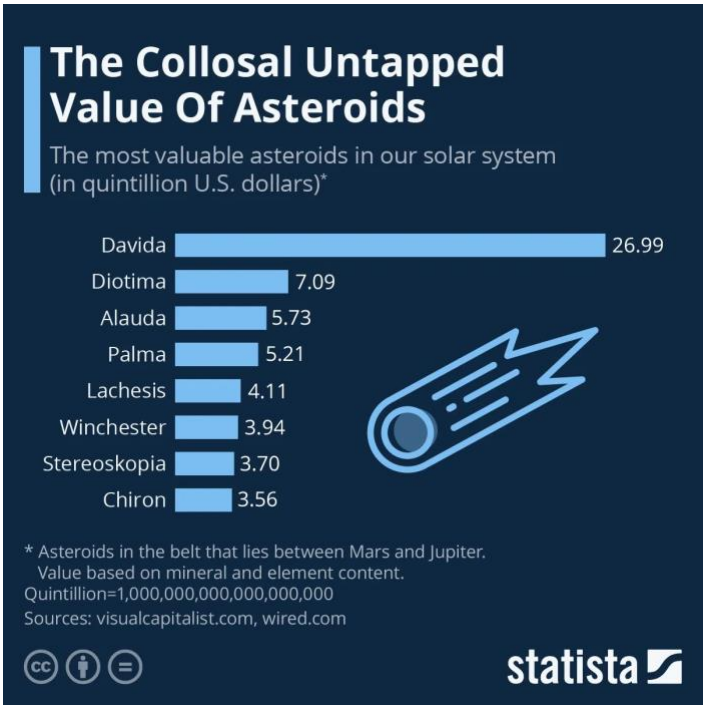

Figure 8: *Infographic taken from Statistas infographic highlighted on the New Space Economy website showcasing the theoretical value in U.S. dollars of minerals found on certain known asteroids.*

The process typically includes identifying and surveying suitable asteroids, followed by deploying robotic spacecraft or autonomous mining systems to the asteroid. These systems could drill into the asteroid, extract the materials, and process them on-site or transport them back to Earth or a nearby space station.

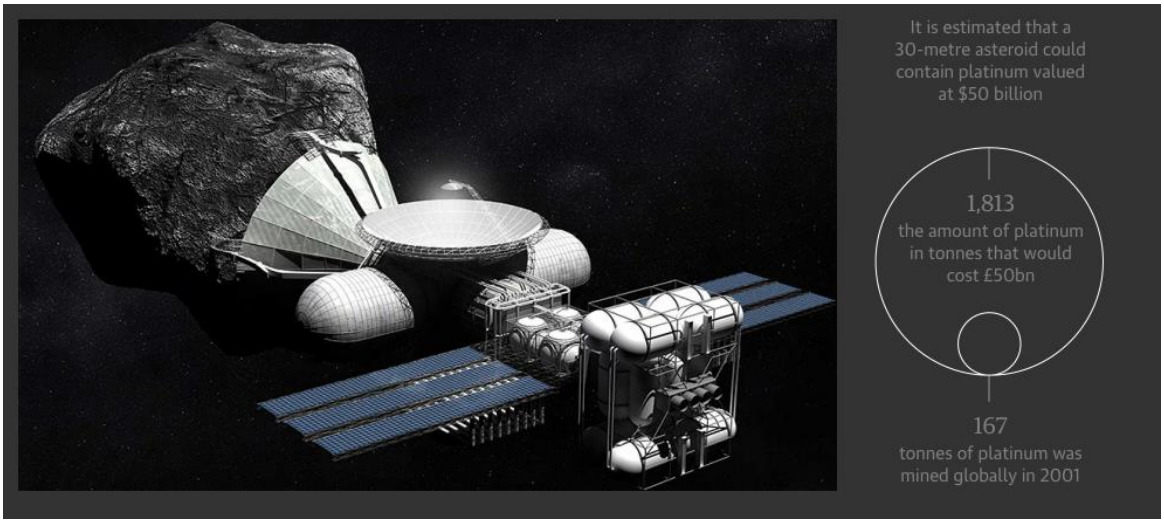

Figure 9: *Graphic taken from an article called "How would asteroid mining work? A visual guide".*

There are asteroid mining companies emerging, such as AstroForge. This company is attempting to launch a refinery into space that would extract minerals from the asteroid, and bring the valuable metals back to Earth. They are targeting ME-type (metallic) asteroids in order to extract platinum group metals. Platinum and iridium found on asteroids are vital raw materials for emerging clean energy technologies.

Figure 10: *Infographic taken from Orbital Today showing a ranking of "Asteroid Mining Companies" in 2023.*

Mining operations have been recognised in the ICARUS Matrix as being a likely target of cyberattacks. Given the immense wealth potential of asteroid mining, intellectual property theft targeting asteroid mining companies is highly likely. These companies, often operating under the protection or backing of their home countries, could also become targets of destructive cyber or physical attacks. Such attacks might be carried out to prevent competitors from gaining a strategic advantage, given the significant economic and geopolitical value asteroid mining could generate.

For instance, the economic benefits of U.S.-based asteroid mining companies would extend beyond tax revenues. The resources extracted could fuel domestic industries, drive technological advancements, and strengthen the nation's global economic position, further amplifying the strategic importance of securing these operations.

Exploration

Uncrewed space exploration missions have been crucial for advancing our understanding of the universe. Various space agencies have launched robotic probes, landers, and rovers that have been sent to study planets, moons, asteroids, and comets.

Notable missions include NASA's Voyager probes exploring the outer solar system, the Spirit and Opportunity Mars rovers studying the Martian surface, and ESA's Rosetta mission to a comet. These are setting the stage for the next phase, crewed space exploration.

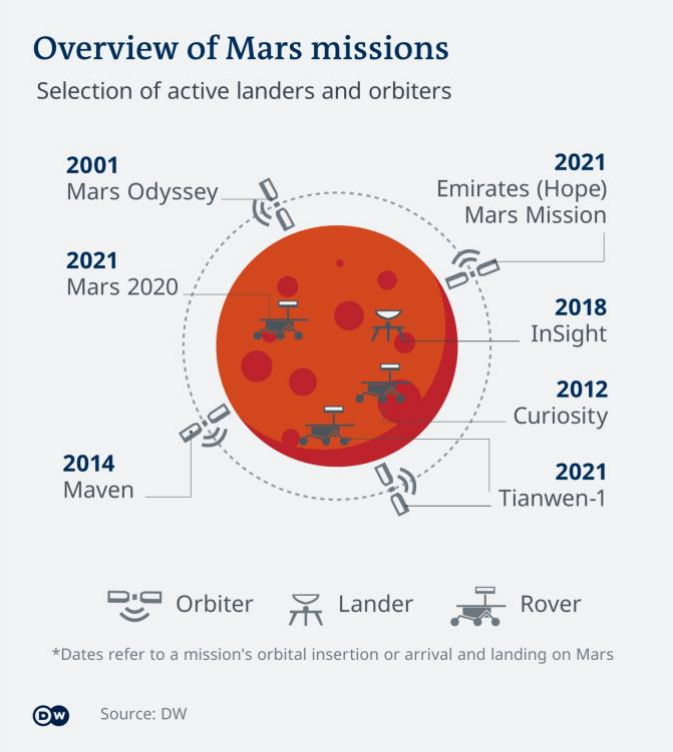

Figure 11: *Infographic taken from Statista's infographic highlighted on DW website showing some of the recent exploration missions to Mars.*

NASA is currently focused on the Artemis programme, and aims to establish a sustainable human presence on the Moon as a precursor to colonising Mars; it aims to put humans on the Red Planet in the 2030s. SpaceX, a private company located in the United States, is actively developing the Starship spacecraft with the ambitious goal of helping to establish a human colony on Mars within the next decade.

China's CNSA plans to explore and potentially colonise the Moon and Mars, with ongoing lunar missions and future Mars expeditions such as the Tianwen-3 Mars sample return mission.

The European Space Agency (ESA) is also exploring Jupiter's moons, focusing on Europa, Ganymede, and Callisto, which are believed to possibly contain oceans. This mission launched in April 2023 and is expected to arrive at Jupiter in July 2031. This was launched using the ESA's Ariane 5 vehicle from Europe's Spaceport in French Guiana.

Planetary exploration is advancing rapidly, and it is increasingly plausible that humans could establish colonies on other planets within the next few decades. As this progress unfolds, nations are likely to intensify cyber espionage efforts to gain an edge in space exploration technologies. Even more concerning is the potential for disruptive or destructive cyberattacks aimed at undermining rival nations' efforts to establish dominance beyond Earth.

The Space Powers

Understanding which nations are participating in the 21st-century space race is crucial, as they are likely to be both prime targets and key perpetrators of cyber-attacks.

Countries with launch capabilities—the ability to design, build, and successfully launch assets into space—are considered space powers. The nations highlighted below not only possess this capability but are also home to prominent private aerospace companies, such as SpaceX in the United States and Antrix Corporation in India. These countries have achieved significant milestones in space exploration, as summarised below, and are expected to accelerate their operations further. To protect their expanding space infrastructure, they are likely to invest heavily in cyber capabilities for both defence and offense.

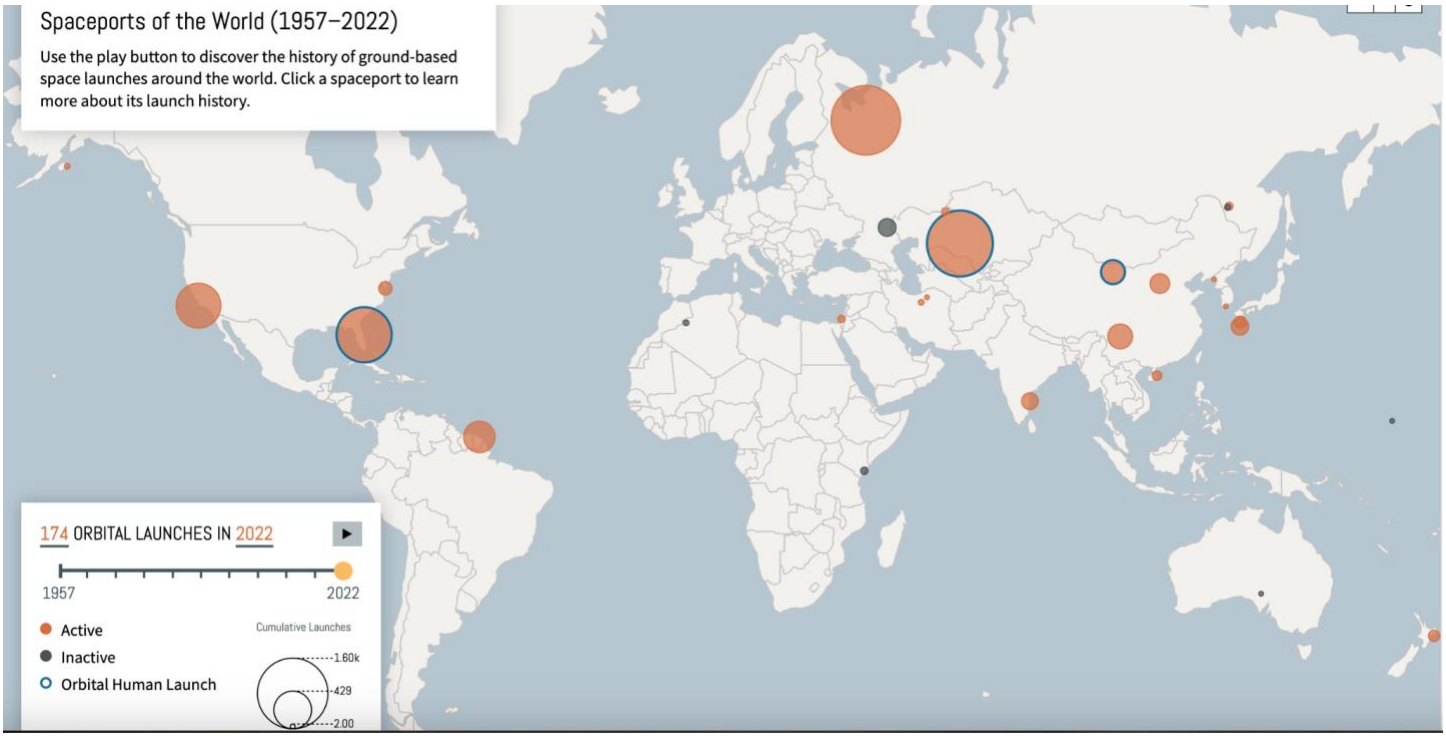

Figure 12: *Global map of spaceports, showing the number of launches throughout 2022. More details of spacesport operations can be found by visiting this website.*

When it comes to what is often referred to as "The Space Race 2.0", the United States and China stand out as clear leaders. Their dominance is underscored by significant investments in space-related startups, driving innovation and advancing key technologies.

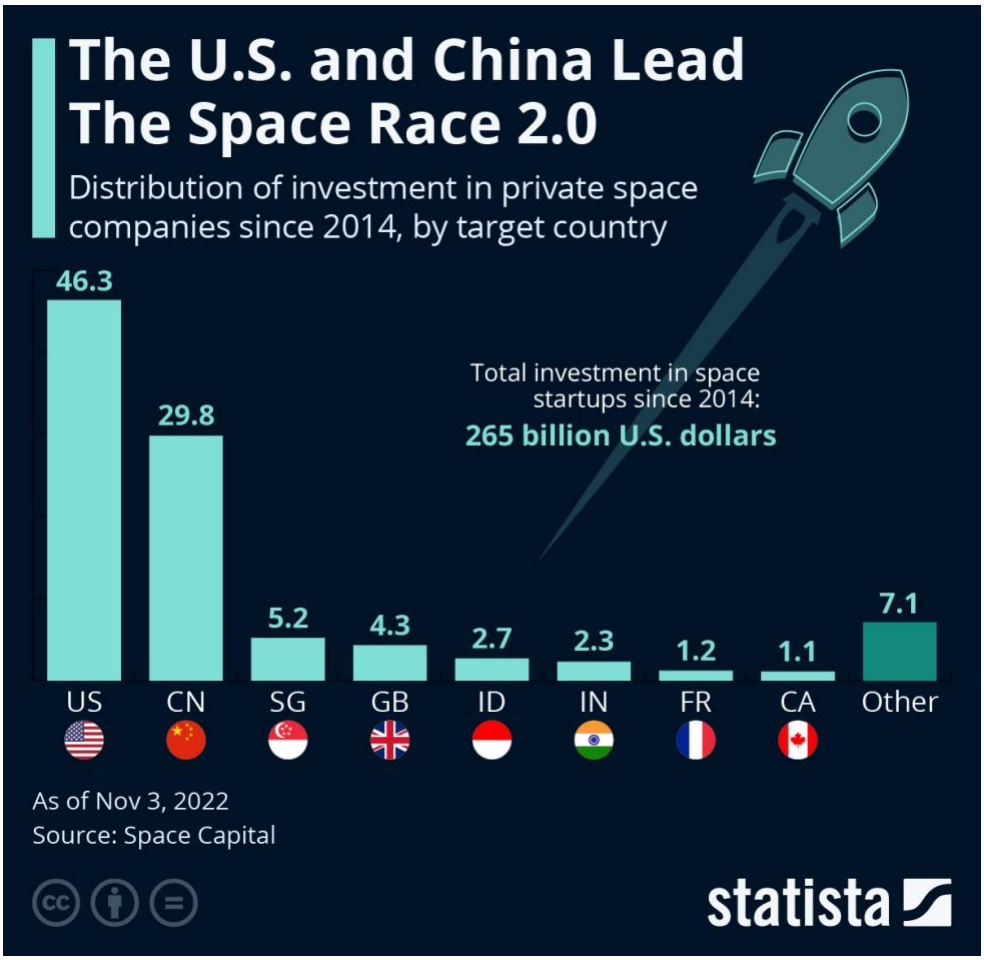

Figure 13: *Investments made by countries in private space companies (2014–2022) in USD.*

If we were to rank the top five space powers based on accomplishments, assets in space, the strength of private and state-owned aerospace industries, ambitions for future missions, and current budgets, a reasonable (albeit subjective) ranking would be as follows:

1. United States
2. China
3. Russia
4. European Union (European Space Agency member states)
5. India

It is important to note that this ranking is dynamic and subject to change as nations' priorities, investments, and technological advancements continue to evolve in the years ahead.

United States: #1

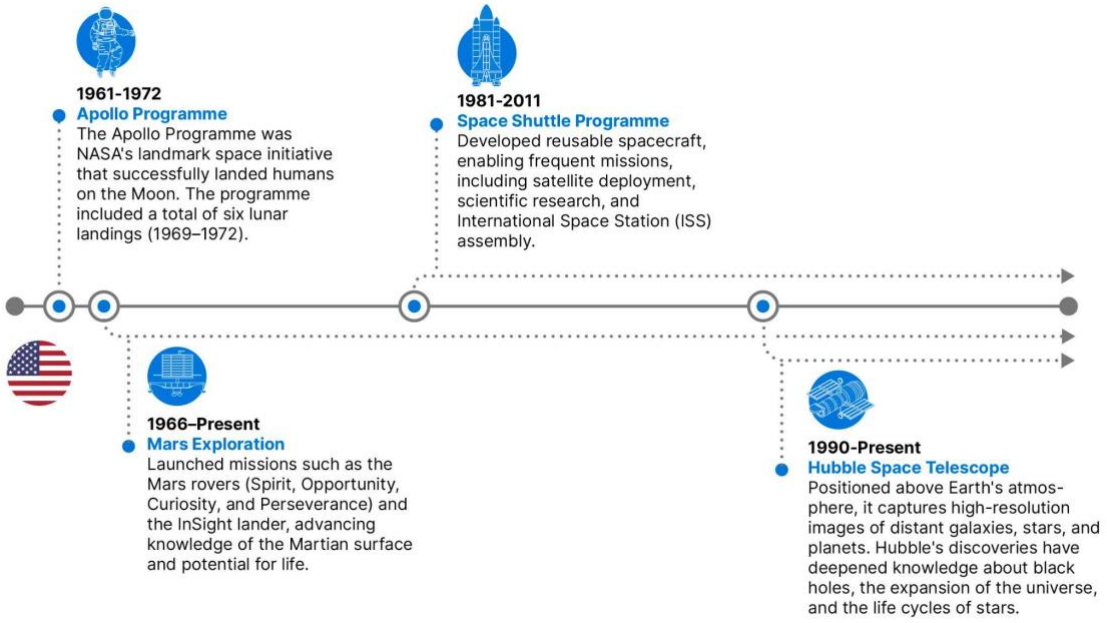

Figure 14: *Summary of key space accomplishments of the United States.*

China: #2

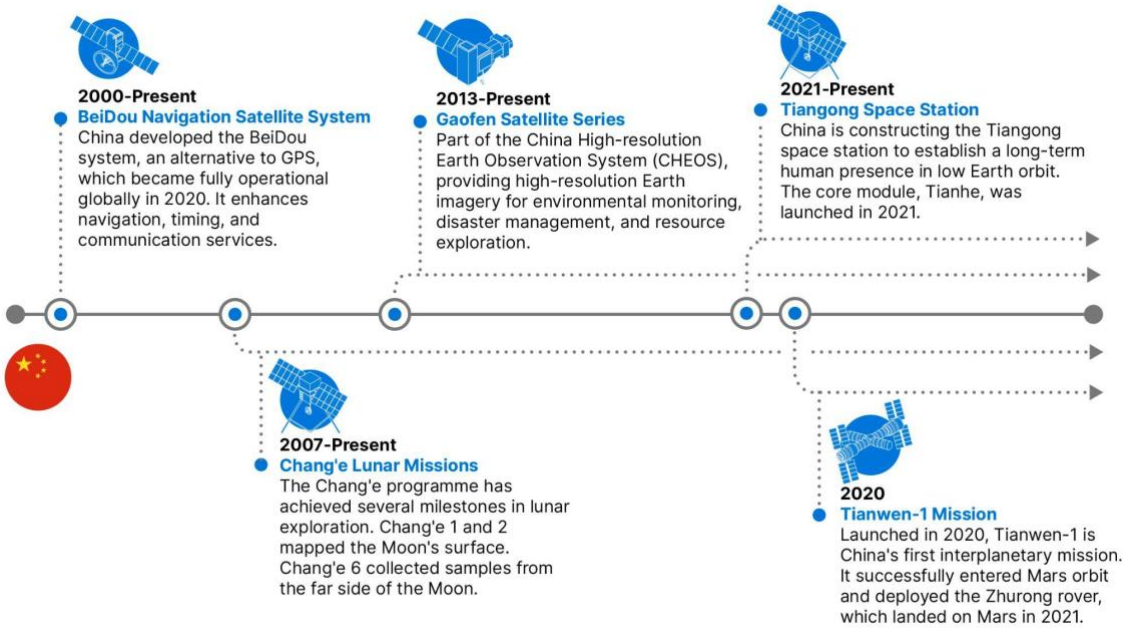

Figure 15: *Summary of key space accomplishments of China.*

Russia: #3

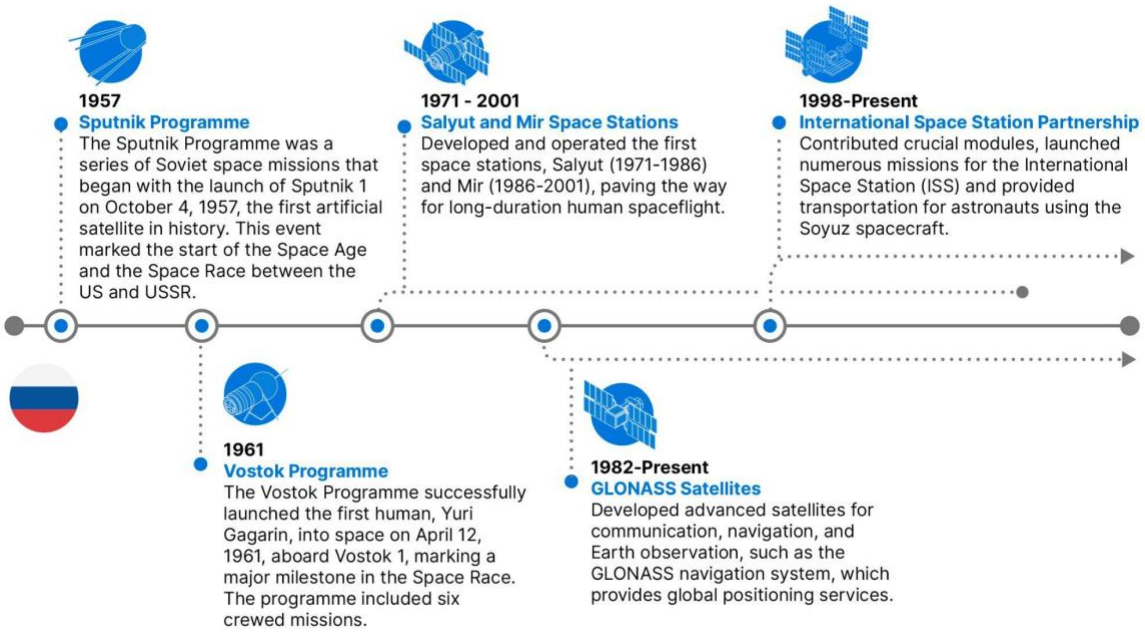

Figure 16: *Summary of key space accomplishments of Russia.*

European Union/ European Space Agency: #4

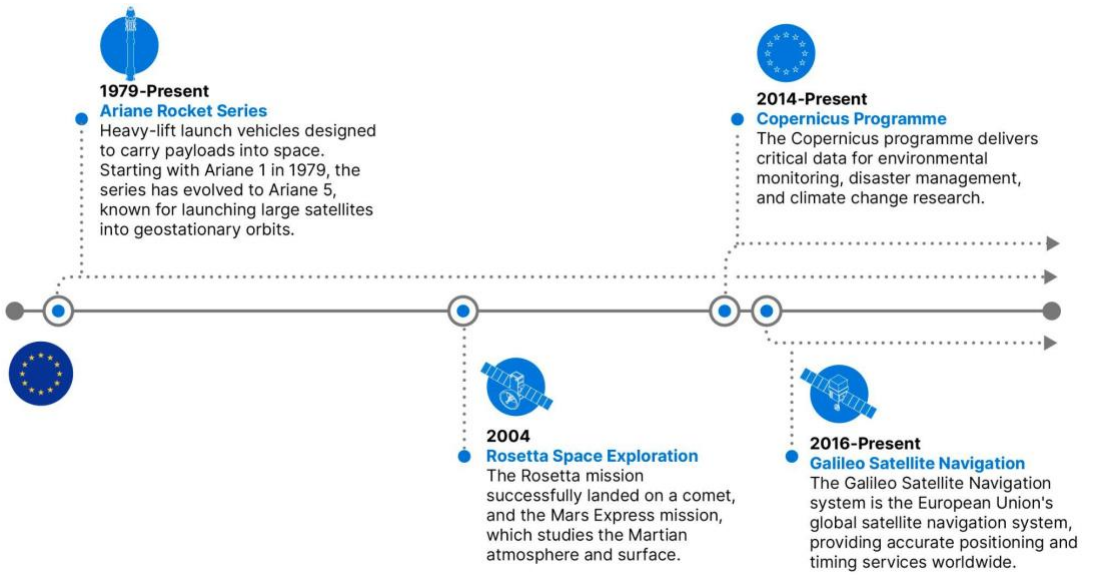

Figure 17: *Summary of key space accomplishments of the European Space Agency.*

India: #5

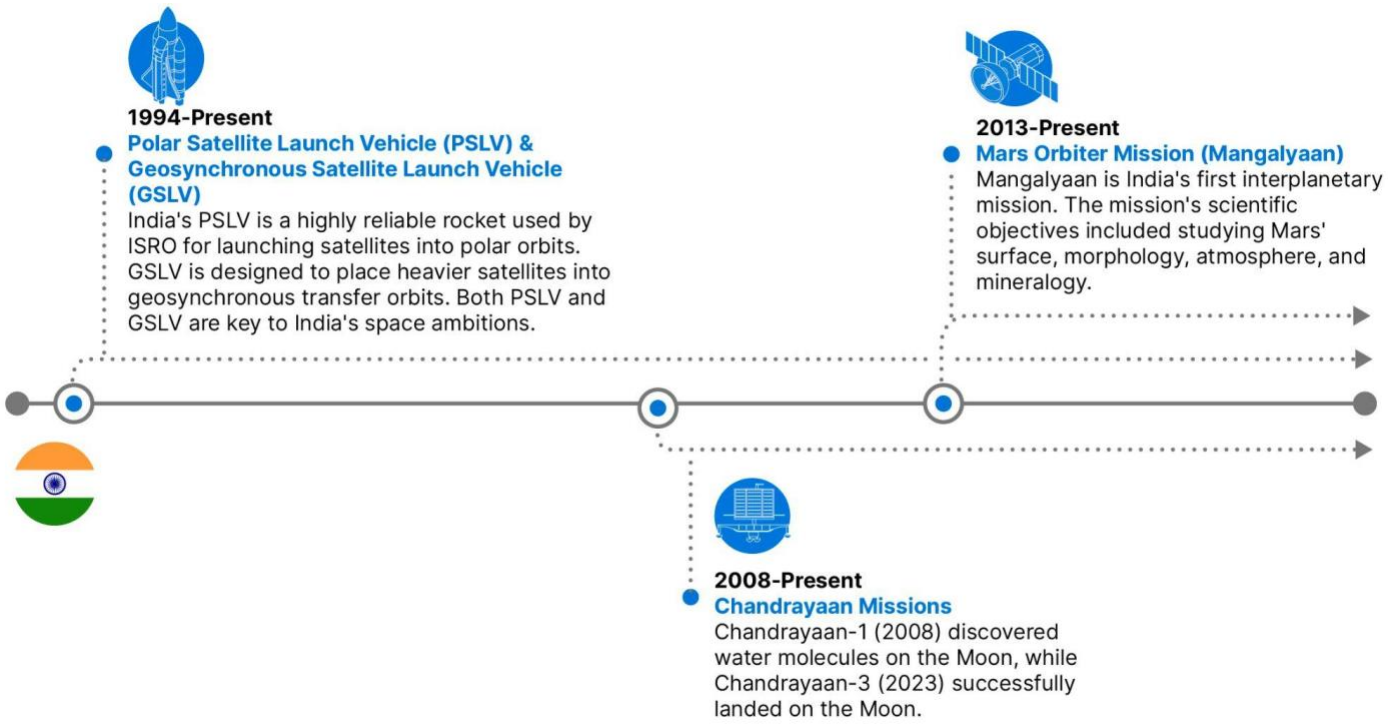

Figure 18: *Summary of key space accomplishments of India.*

Emerging

There are also nations with big aspirations in space, below are some of the most significant emerging space powers to keep a close eye on.

Japan: The Japan Aerospace Exploration Agency (JAXA) leads with advanced missions, including the Hayabusa asteroid missions and lunar exploration initiatives. Japan successfully landed the Hayabusa2 spacecraft on an asteroid and returned samples to Earth, and is advancing lunar exploration ambitions.

United Arab Emirates: The UAE Space Agency oversees ambitious projects like the Mars Mission Hope and aims to advance space science and technology in the Middle East. Its Hope Probe entered Mars orbit in 2021, providing valuable data about the atmosphere and climate. The UAE plans to expand its space programme and develop a robust space industry.

Israel: The Israel Space Agency (ISA) has made strides with satellite technology and attempted lunar missions, including the Beresheet lander. The Beresheet lander, despite its crash-landing clearly demonstrated Israel's capability to reach the Moon, while the country continues to advance satellite technology. Israel will likely continue to focus on space technology innovation and international collaborations.

South Korea: The Korea Aerospace Research Institute (KARI) drives space efforts with satellite launches and plans for lunar exploration, such as the Korea Pathfinder Lunar Orbiter. KARI launched its first domestically-built satellite into space and is working on lunar exploration. South Korea aims to develop advanced satellite technology and strengthen its space industry through domestic and international partnerships.

Artemis Accords

The Artemis Accords are a U.S.-led initiative designed to promote the peaceful exploration and commercial use of space. Announced in 2020 by NASA and the U.S. Department of State, these non-binding agreements aim to establish principles for responsible space activity.

Notably, China and Russia have declined to sign the Accords, signaling the emergence of two distinct blocs in the new space race. One led by the United States and its allies, and the other centered around China, with Russia aligning closely with Beijing.

***Figure 19**: Panama and Austria signing the Artemis Accords in December 2024.*

Militarisation of Space

Space has been militarised for decades, primarily by the United States and Russia. However, the pace of militarisation has significantly accelerated, with new nations increasingly expanding their operations into space. This trend carries two

key implications. First, the potential for conflict is extending beyond Earth's surface. Second, many of the countries advancing their military presence in space also possess considerable cyber capabilities—most notably the United States, China, and Russia. In particular, the United States and China appear to be aligning their cyber and space capabilities, integrating them closely for strategic purposes. We will examine specific examples of this alignment in more detail.

The militarisation of space is a trend that is almost certain to accelerate, and it is highly likely that more nations will combine their cyber and space capabilities for both defensive and offensive operations. Given this trajectory, it is essential to highlight some of the key space forces and commands that are emerging globally.

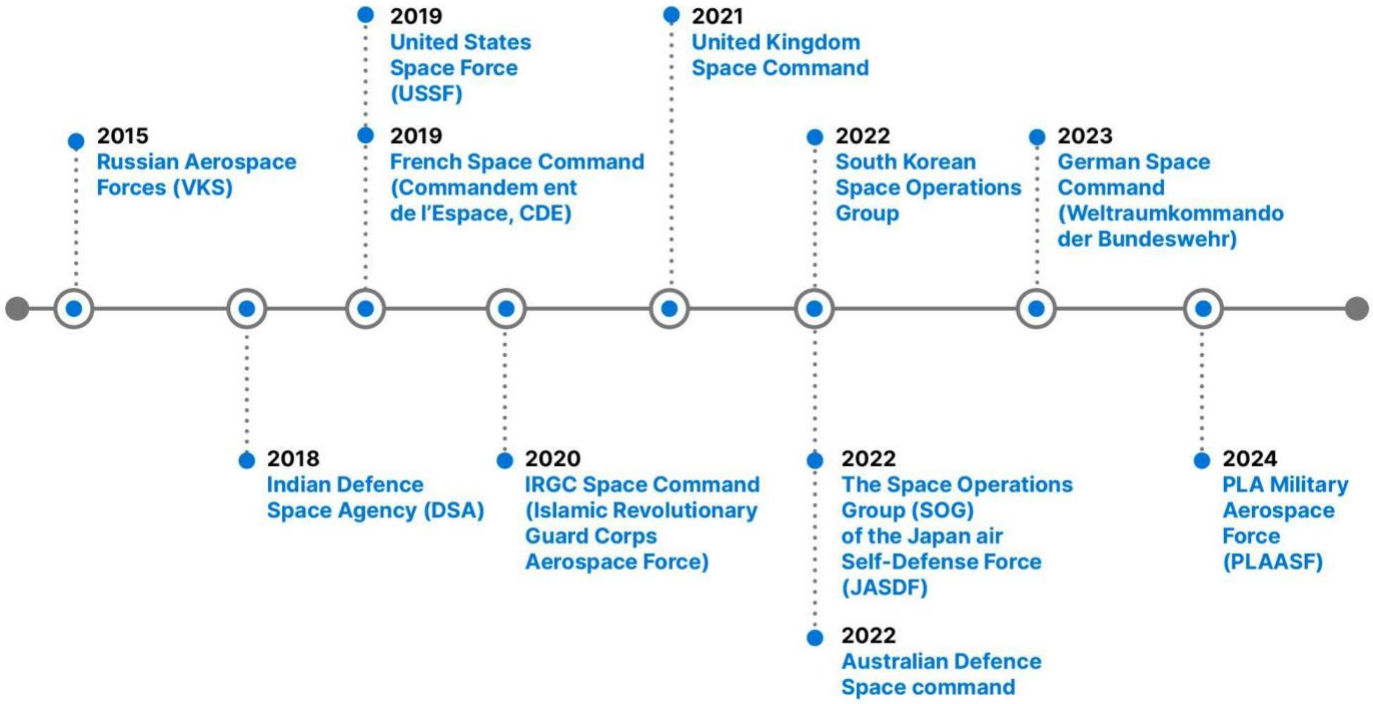

***Figure 20**: Summary of 11 countries with space-related military organisations. List is not exhaustive; many countries are developing nascent space capabilities from their Air Forces.*

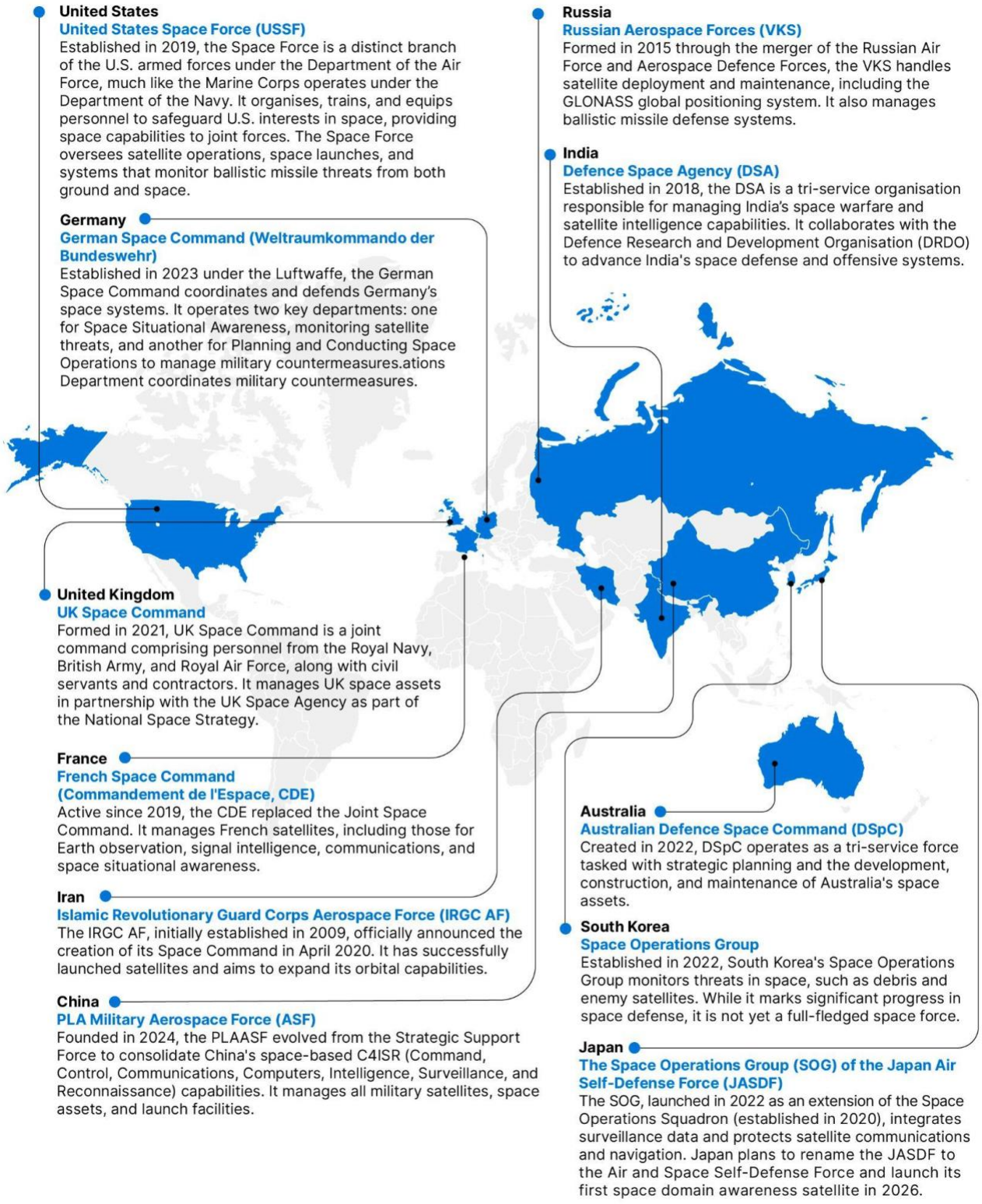

***Figure 21**: This summary highlights 11 countries with established space-related organisations. The list is not exhaustive, as many nations are advancing space capabilities, often within their Air Forces.*

United States

The United States Space Force (USSF) was officially established on December 20, 2019, as the sixth branch of the U.S Armed Forces. It was created in response to growing concerns about the security and strategic importance of space, recognising that space has become a critical domain for national defence, similar to land, sea, air, and cyberspace.

***Figure 22**: Image of "U.S Space Force Guardians participate in Moonlighter, an exercise designed to focus on refining the defensive and offensive skill sets of Cyber Guardians, centered around the Moonlighter imaging satellite, in Colorado Springs, Colorado, Nov. 15, 2023, The Moonlighter imaging satellite, a 3U CubeSat, serves as an exclusive on-orbit cyber test platform. Its role includes facilitating defensive cyber operations and refining cyber-related tactics, techniques, and procedures".*

Space Delta 6 in particular "executes cyber operations to protect space operations…". Furthermore, Space Delta 7 "provides intelligence data to allow for the detection and characterisation of adversary space capabilities". An element of cyber capability is probably included here also given documented reporting of US cyber capabilities. This is important because it reinforces the argument that space and cyber capabilities are increasingly becoming intertwined.

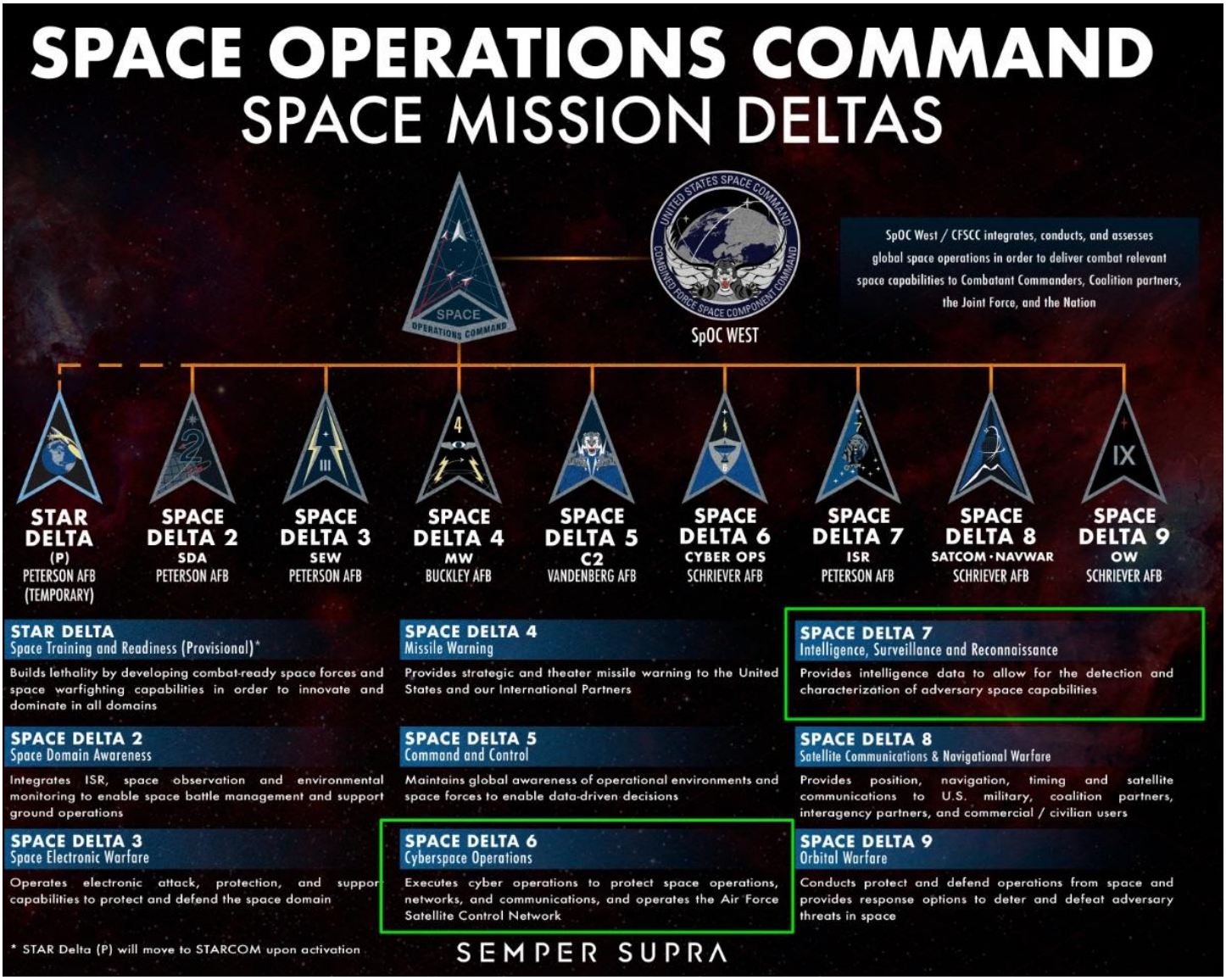

***Figure 23**: Summary of United States Space Operations Command and Space Mission details.*

China

Since 2015, China has been developing and deploying near-space flight vehicles (NSFVs)—including balloons, aerostats, and hypersonic platforms—to bolster its military intelligence, surveillance, and reconnaissance (ISR) capabilities. According to a 2023 Insikt report, the People's Liberation Army (PLA) almost certainly operates a fleet of NSFVs, integrated with satellites and other collection systems to enhance its strategic intelligence network.

In April 2024, China established the People's Liberation Army Aerospace Force (PLAASF), underscoring its strategic emphasis on advancing space operations. The PLAASF is tasked with achieving and maintaining space dominance, safeguarding China's space assets, and ensuring unimpeded operations in the space domain.

Complementing the PLAASF are the PLA Cyberspace Force (PLACSF) and the PLA Information Support Force (PLAISF). These forces are likely responsible for conducting both offensive and defensive cyber operations, further strengthening China's integrated approach to modern warfare.

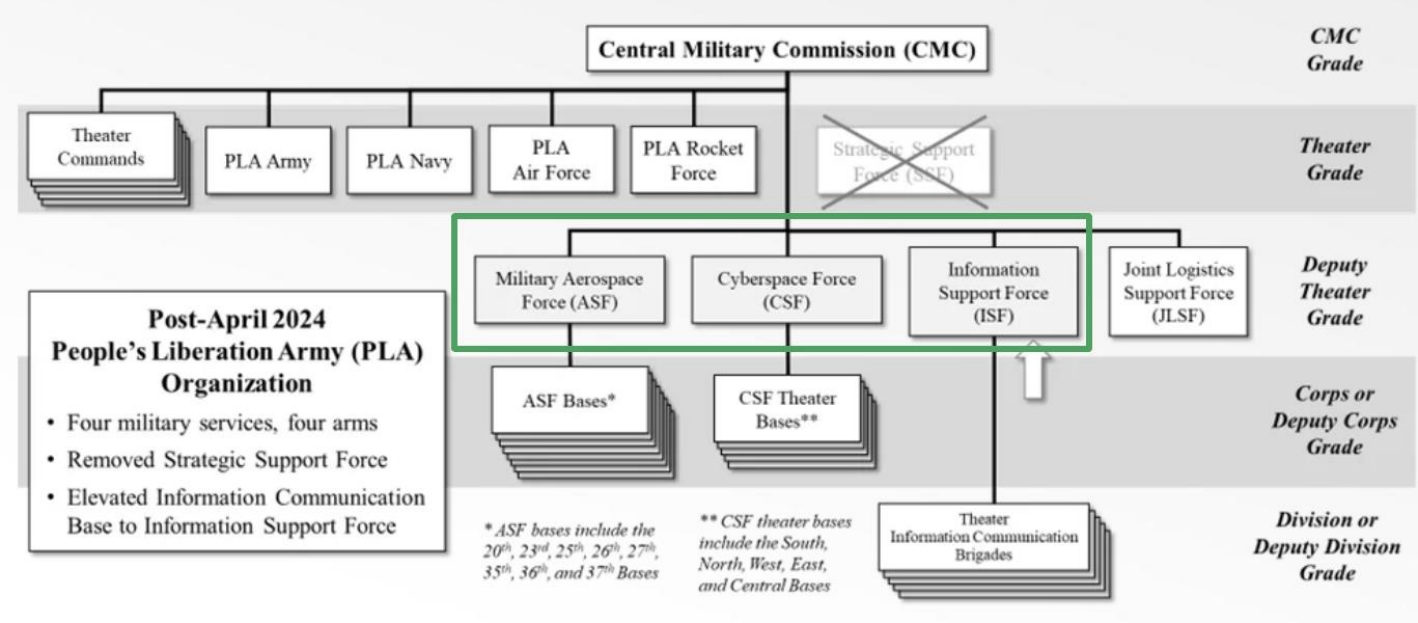

***Figure 24**: The Military Aerospace Force (ASF), established in April 2024, operates alongside China's advanced cyber capabilities, including the Cyberspace Force (CSF) and the Information Support Force (ISF).*

Before the 2024 reforms, the PLA's Strategic Support Force (SSF), created in late 2015, comprised two key branches: the Network Systems Department (NSD) and the Space Systems Department (SSD). The integration of these branches highlights China's recognition of the critical link between space and cyber domains. This alignment underscores the strategic importance of protecting space assets from cyber threats while potentially leveraging cyber operations to disrupt the space capabilities of adversaries

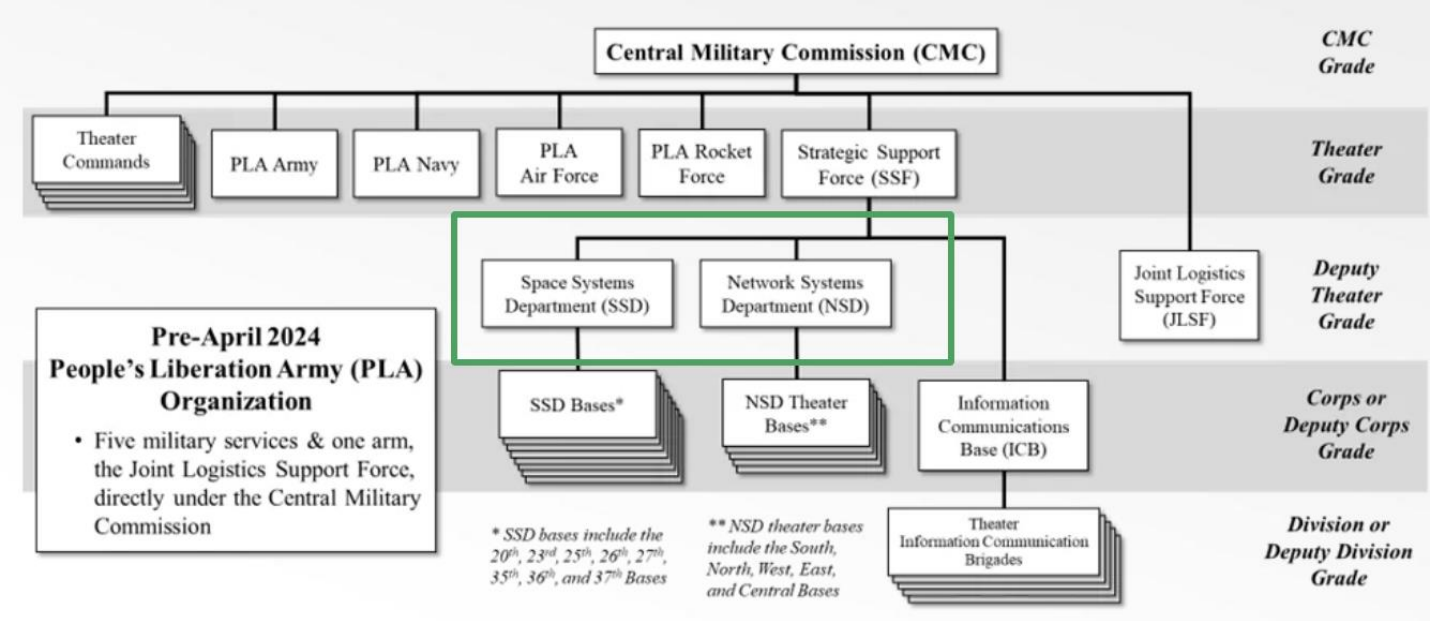

***Figure 25**: Summary of the old structure of the PLA Strategic Support Force (PLASSF).*

According to the report, China is advancing its development of satellite "inspection and repair" systems, which have the potential to function as weapons. This was exemplified in 2022 when the Shijian-21 satellite maneuvered a defunct satellite into a graveyard orbit above GEO, showcasing technology that could be adapted to grapple with and disable other satellites in the future.

The PLA is also equipped with ground-based laser weapons capable of disrupting or damaging satellites, with plans to develop even more powerful systems by the mid-to-late 2020s. Additionally, PLA military exercises routinely feature jamming technologies targeting space-based communications, radar, and navigation systems, including U.S. military SATCOM operating at protected frequencies.

Russia

Russia has intensified its focus on militarising space as a key element of its national security strategy. This focus is reflected in the establishment of the Russian Aerospace Forces (VKS) in 2015, further consolidating its space capabilities. While the VKS does not explicitly include dedicated cyber units, it is likely supported by Russia's broader military cyber efforts, indicating an integrated approach to space and cyber operations.

Russia's advancements in anti-satellite (ASAT) technology have raised concerns in the United States. Notably, Moscow tested the Nudol missile in 2021, capable of destroying satellites in low Earth orbit. In May 2024, the U.S. accused Russia of launching a satellite suspected of being able to attack other satellites, further heightening tensions. Such developments underscore Russia's commitment to enhancing its space warfare capabilities, posing significant challenges to global security in the space domain.

Figure 26: *Image of Russia likely testing its 14Ts033 Nudol (PL-19) kinetic interceptor missile system.*

Russia's space programme has faced significant setbacks due to its ongoing war in Ukraine. International sanctions have restricted access to critical electronics and components within the supply chain, hindering progress. As a result, Russia may increasingly turn to China for support, potentially deepening collaboration in future space operations to achieve its strategic ambitions.

Cyber Threats to Space

The aerospace sector is facing an accelerating wave of cyberattacks, in parallel with advancements in space-related technologies. Nation-state actors continue to prioritise the theft of intellectual property to bolster their space programmes. However, since the late 2010s, there has been a notable rise in more malicious cyberattacks carried out by both state-sponsored groups and criminal organisations.

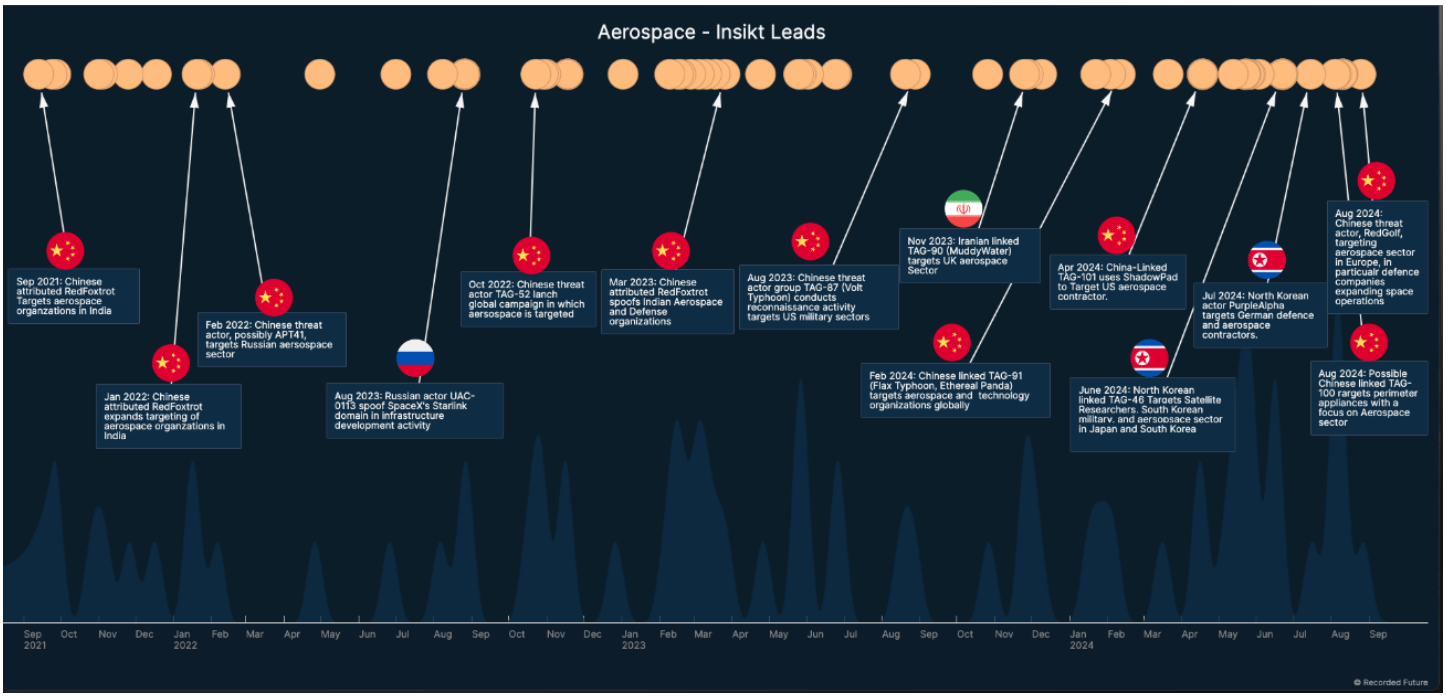

Figure 27: *Timeline of Recorded Future Insikt Research Leads, which are not publicly available, showing some key nation-state targeting of the aerospace sector from September 2021 to September 2024.*

In response to this growing threat, operational-level cyber risks to space assets have been mapped in the SPARTA matrix. This matrix aligns with the widely recognised MITRE ATT&CK framework, commonly used by cybersecurity professionals, providing a structured approach to understanding and mitigating cyber threats in the space domain.

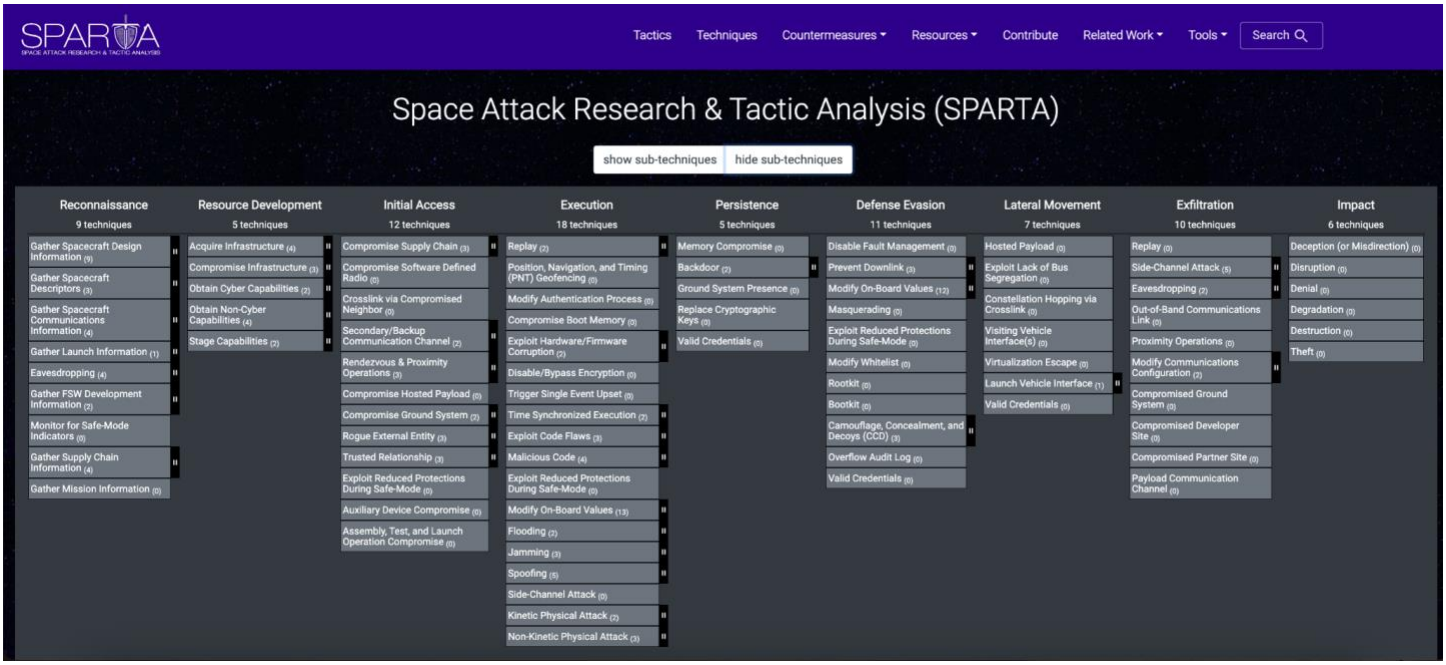

Figure 28: *https://sparta.aerospace.org/*.

Cyberattacks on space systems have been occurring since the mid-1980s, targeting government, commercial, and scientific operations alike. According to a report by Deloitte, space systems face vulnerabilities across five critical segments: space (satellites), ground (infrastructure), user (devices like GPS), link (communications networks), and launch (launch-related components). Each of these segments is vital to space operations but also represents a potential entry point for cyber threats.

When examining a satellite in its simplest form, it becomes evident that it has numerous points of vulnerability, particularly during its construction or when connected to terrestrial systems. A satellite can even be likened to an Internet of Things (IoT) device, with similar risks of exploitation. The graphic below highlights the key components of a satellite, showcasing the areas most susceptible to cyber threats.

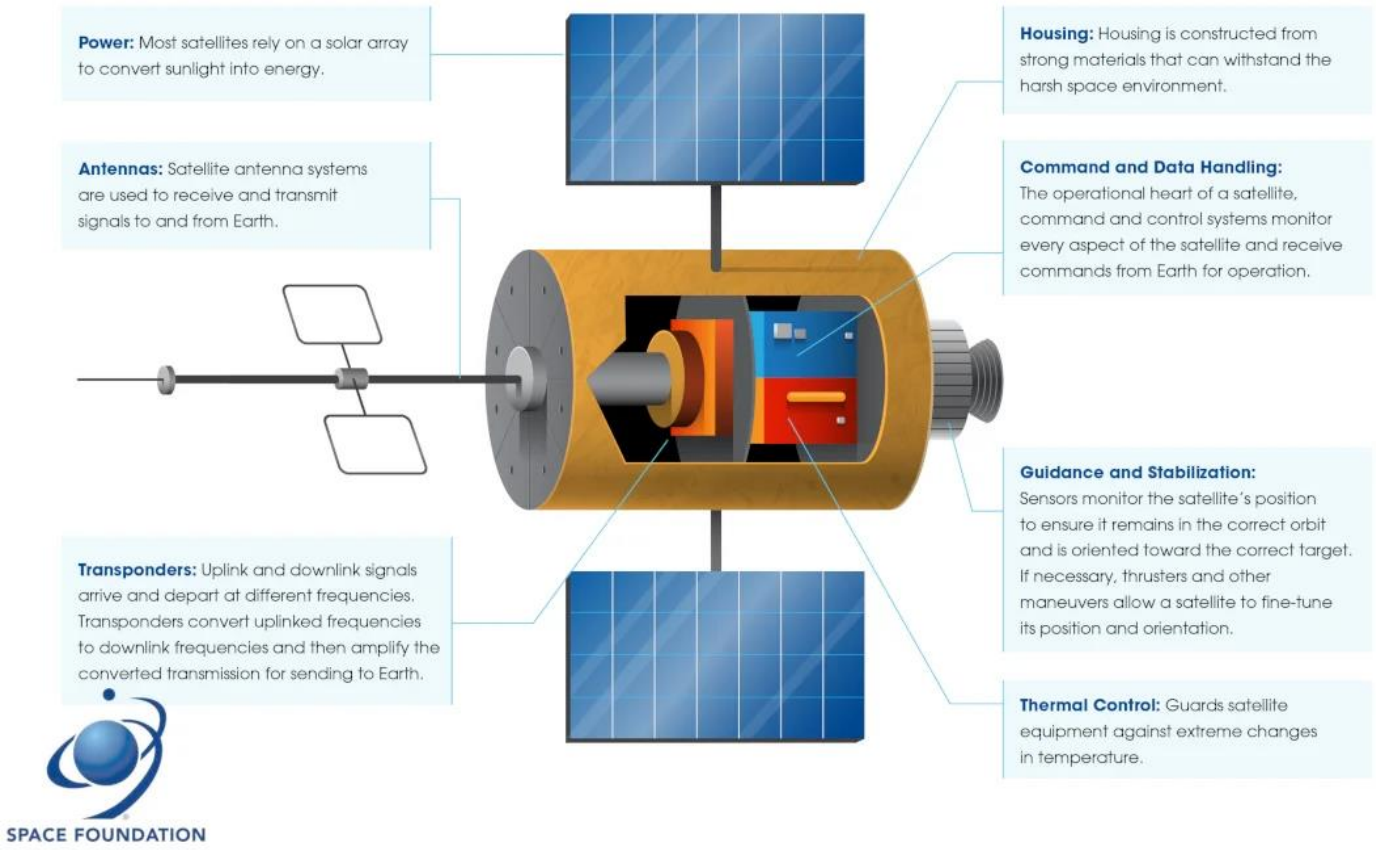

Figure 29: *Components commonly found on most satellites.*

In the following section, we will categorise space-related cyber threats into four key areas: espionage, signal hijacking, destructive attacks, and supply chain attacks. For each category, we will examine real-world examples of past cyber incidents or potential vulnerabilities that could be exploited in the future.

Espionage

The space industry has become a prime target for nation-state espionage. In 2023, the FBI and U.S. Air Force issued a joint advisory highlighting a surge in cyber-espionage attacks targeting U.S.-based space companies. According to the advisory, the global space economy is projected to exceed $1 trillion by 2030, with the U.S. and China leading in space equity investment. This competitive dynamic makes it likely that most cyber-espionage efforts will originate from or target these two nations.

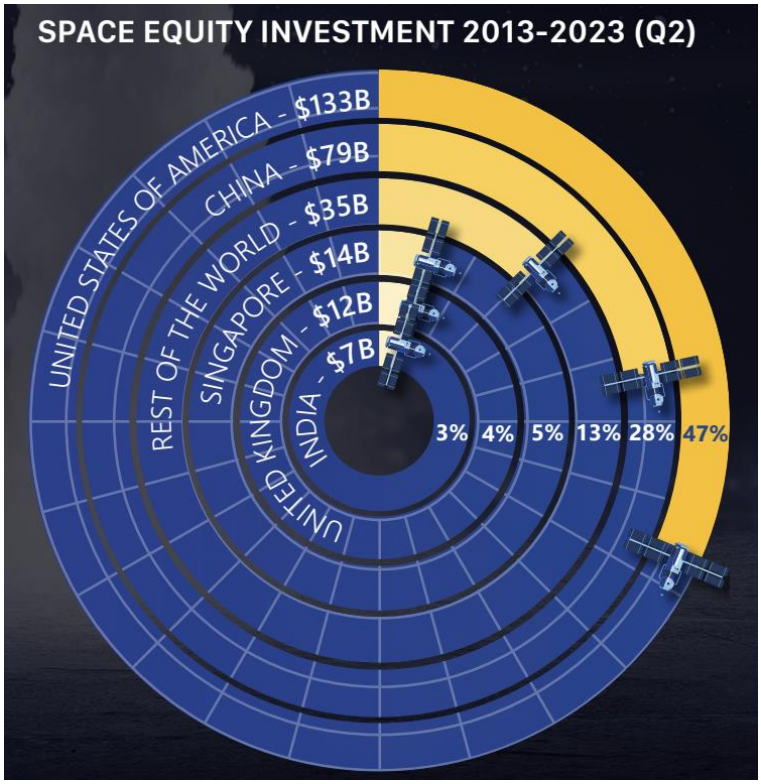

Figure 30: *Space equity investment trends from 2013 to 2023, as reported in the U.S. advisory.*

In 2018, two hackers associated with China's Ministry of State Security were charged with stealing sensitive digital data from NASA's Jet Propulsion Laboratory (JPL). JPL, renowned for its leadership in robotic space exploration, has been instrumental in missions such as sending rovers to Mars and deploying satellites and probes into space.

More recently, in 2023, Chinese hackers were accused of breaching the Japan Aerospace Exploration Agency (JAXA), stealing over 10,000 files containing classified information. The attackers reportedly exploited vulnerabilities in JAXA's

virtual private networks (VPNs). This was not an isolated incident, JAXA had also been targeted by Chinese threat actors in 2013 and 2016.

In 2022, Fancy Bear, a cyber-espionage group associated with Russia's GRU military intelligence agency, reportedly infiltrated U.S. satellite networks. By exploiting an unpatched 2018 vulnerability in a virtual network, the group was able to capture credentials during active sessions. This attack targeted critical satellite communications relied upon by the military and other government entities. The incident exposed significant weaknesses in satellite infrastructure and emphasised the strategic risks of cyberattacks on space assets, particularly during periods of geopolitical tension. It also fueled calls to classify space technology as critical infrastructure, a designation that would grant the industry expanded access to intelligence-sharing mechanisms and disaster planning resources.

Figure 31: *FBI Wanted List of GRU hackers targeting the United States.*

In 2024, Trend Micro reported on the TIDRONE threat cluster, which has been linked to Chinese-speaking threat actors. This cluster targeted Taiwan's military-related industries, including those involved in satellite production, by exploiting vulnerabilities in ERP software and remote desktops. TIDRONE deployed sophisticated malware such as CXCLNT and CLNTEND, capable of collecting data, dumping credentials, and disabling antivirus systems. This campaign appeared to be focused on espionage, with evidence suggesting a potential supply chain compromise as the entry point for the intrusions.

Signal Hijacking

Over the past decade, incidents of signal hijacking linked to Russia have surged. In 2024, the United Nations' telecommunication agency publicly condemned Russia for interfering with satellite systems across several European countries, calling for an immediate cessation of these activities. This condemnation followed formal complaints from Ukraine, France, Sweden, the Netherlands, and Luxembourg regarding disruptions to GPS signals and television broadcasts.

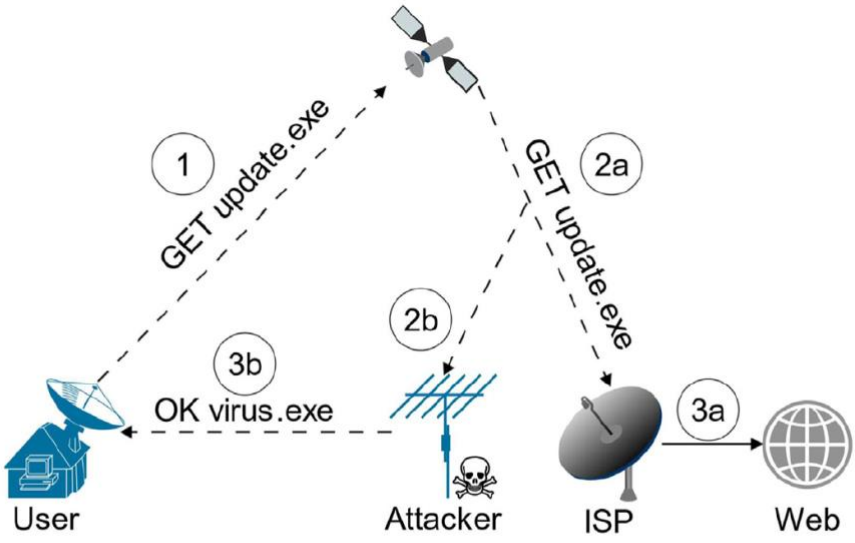

Figure 5: Demonstrative signal injection attack. At time 1 in the figure, the user requests a secure download file from a trusted server. Both the ISP (2a) and the eavesdropper (2b) receive this transmission concurrently. While the ISP routes the request over the Internet (3a), the attacker transmits a malicious response to the customer antenna (3b).

Figure 32: *High-level depiction of how a cyber threat actor can hijack a satellite signal to inject malware into a victim's device.*

One of the most notorious instances of combining signal hijacking with a cyber threat campaign was the Turla operation, reported by Secure List in 2015 in an article titled "Satellite Turla: APT Command and Control in the Sky."

In this operation, the Turla group exploited satellite communication systems to conduct sophisticated cyberattacks. They hijacked the downlink frequencies of poorly secured commercial satellites to create command-and-control (C&C) infrastructure, enabling them to manage malware infections and exfiltrate data from compromised systems. After identifying an IP address routed through a satellite's downstream link, Turla monitored packets from the internet destined for this IP.

Researchers noted that this method of using hijacked downstream-only links was both cost-effective and relatively straightforward. Maintaining such an operation cost approximately USD 1,000 per year and provided an efficient means of managing malware and communicating with victim machines.

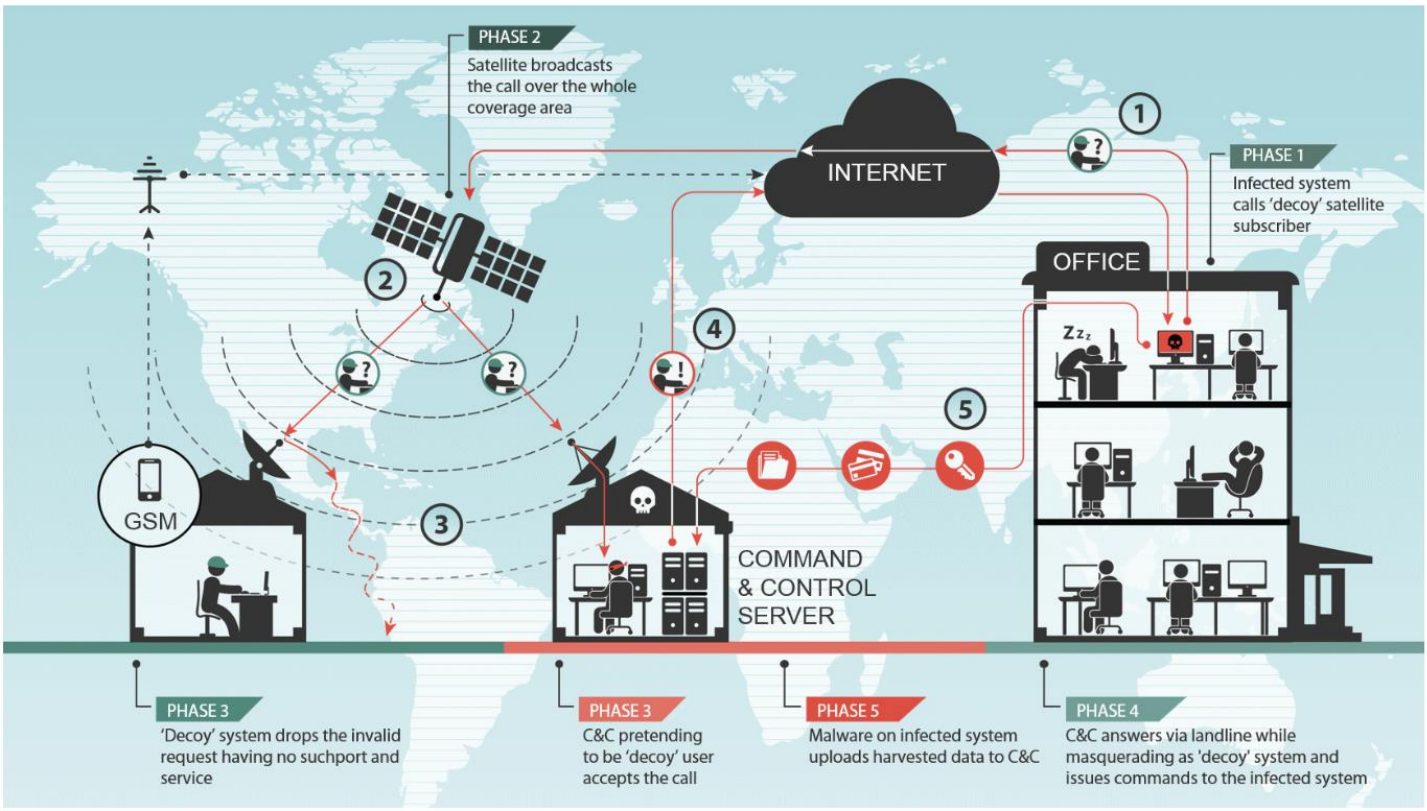

Figure 33: *Summary of how satellite internet hijacking works in SecureList's report.*

It is worth noting that Turla is not the only group known to exploit similar methods. The report highlights that the now-defunct company HackingTeam and the Iranian-affiliated group Rocket Kitten have also employed satellite-based internet links for their operations.

Signal hijacking has also been utilised for information operations. In May 2024, hackers targeted Astra communication satellites, owned and operated by the Luxembourg-based company SES. By transmitting a stronger signal, they were able to override broadcasts on at least 15 television channels, replacing them with footage of Moscow's Victory Day parade—an event commemorating the defeat of Nazi Germany in World War II. This incident affected Ukraine, as well as numerous countries across Europe and the Baltics.

Destructive

The number of vulnerabilities that a space asset could be exposed to is significant. So much so that annual gatherings such as CYSAT have emerged. Since 2021, this event has brought together "all the players in the space cybersecurity domain" with the mission of "Raising awareness about cybersecurity for space assets and data".

Space assets face a wide array of vulnerabilities, prompting significant attention from the cybersecurity community. This concern has led to the establishment of annual gatherings like CYSAT, which since 2021 has brought together "all the

players in the space cybersecurity domain." It has the mission of "Raising awareness about cybersecurity for space assets and data".

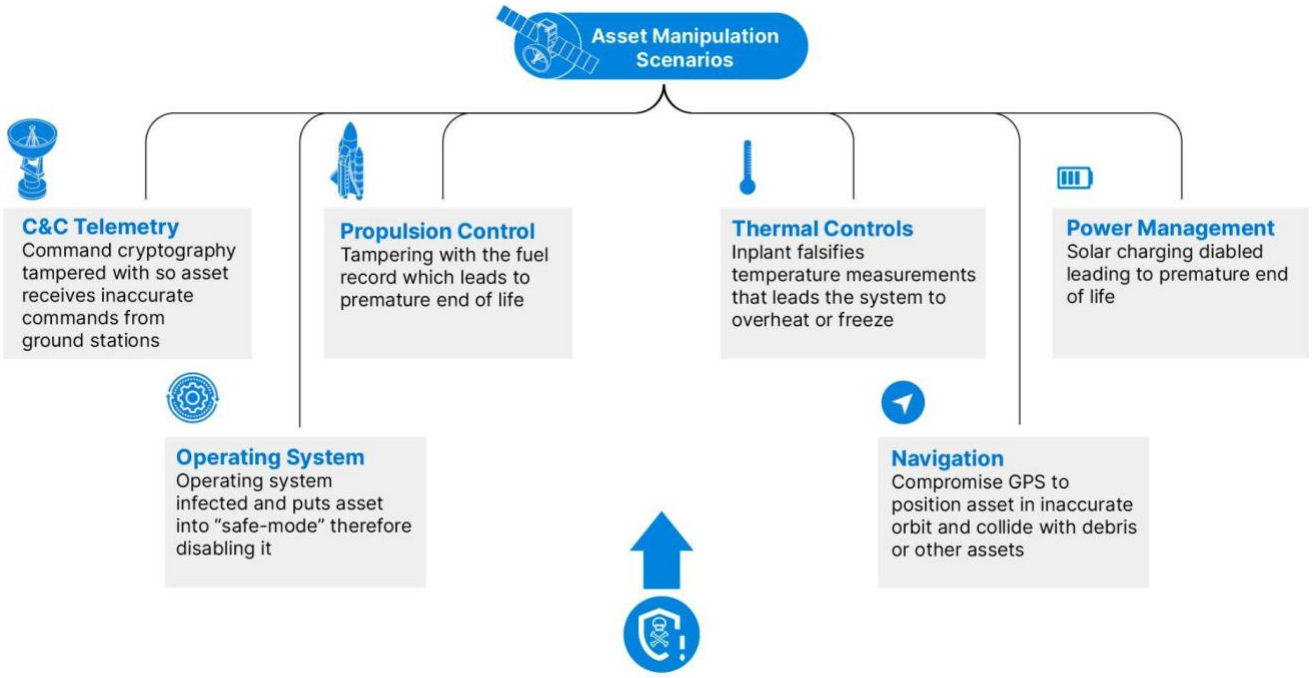

Figure 34: *Graphic illustrating potential vulnerabilities in space assets that could be exploited by threat actors.*

In 2021, the South African National Space Agency (SANSA) fell victim to a breach orchestrated by CoomingProject, a criminal group believed to have Russian origins. The attackers reportedly stole 20GB of data, which was subsequently leaked online. SANSA stated that most of the leaked data consisted of space-related research already available in the public domain. The attackers did not disclose the specific vulnerability they exploited to access SANSA's systems and file server.

Figure 35: *Screenshot of CoomingProject's announcement of the SANSA compromise, including a hyperlink to the stolen data.*

The following year, in 2022, a cyberattack targeted the Atacama Large Millimeter/submillimeter Array (ALMA), one of the world's most advanced astronomical observatories, located in Chile. The attack forced ALMA to suspend its scientific operations temporarily, disrupting critical data collection and processing systems. Additionally, the observatory's website went offline. Although the perpetrators were never identified, speculation points to a ransomware group as the likely culprit.

A more notorious example of a destructive attack on space-based assets occurred on February 24, 2022, the day Russia launched its full-scale invasion of Ukraine. Viasat, a U.S.-based satellite communications company, was targeted in a cyberattack that appeared designed to disrupt Ukrainian communications as part of the military campaign. The attackers exploited a misconfigured VPN device to gain unauthorised access to the KA-SAT satellite network's ground-based modems. They then issued destructive commands to tens of thousands of modems, causing widespread service outages across Ukraine and parts of Europe. The attack also disrupted critical infrastructure, such as wind farms and internet services in remote regions, as well as the Ukrainian military's communications capabilities.

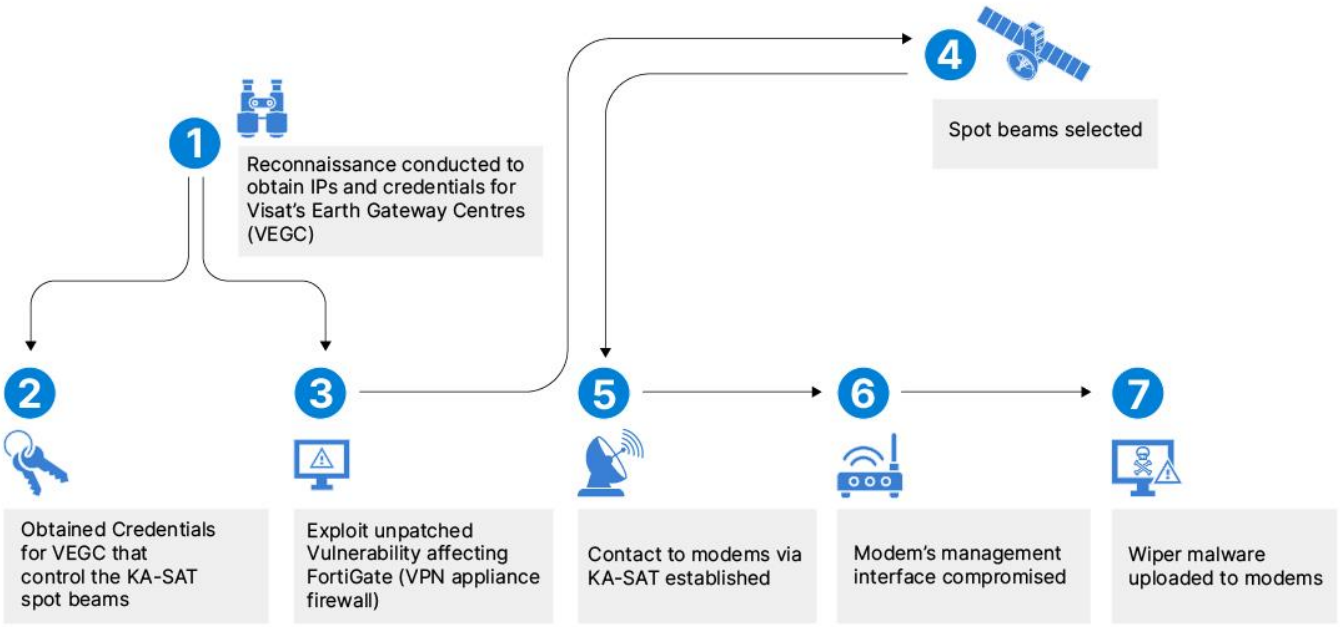

Figure 36: *Summary of Visat attack.*

In mid-2023, hackers successfully disrupted the operations of Dozor-Teleport, a subsidiary of the state-owned Russian Satellite Communications Company (RSCC). The attackers launched a Distributed Denial of Service (DDoS) attack that overwhelmed Dozor-Teleport's networks with an enormous volume of traffic, causing widespread disruptions to its services. The responsible group claimed not only to have disrupted communications but also to have gained access to internal systems, exfiltrated sensitive data, and damaged user terminals.

In 2024, research conducted by VisionSpace Group revealed critical vulnerabilities in NASA's CryptoLib v1.3.0, a library used to secure spacecraft communications. The identified flaws could cause segmentation faults, potentially crashing onboard systems and ground stations. Proof-of-Concept (PoC) exploits demonstrated attacks on AOS, TM, and TC frames, resulting in denial-of-service (DoS) conditions. The vulnerabilities were traced to unchecked Security Parameter Index (SPI) values, which could lead to invalid memory access. To mitigate these risks, the research recommends validating SPI values before dereferencing pointers to ensure robust security.

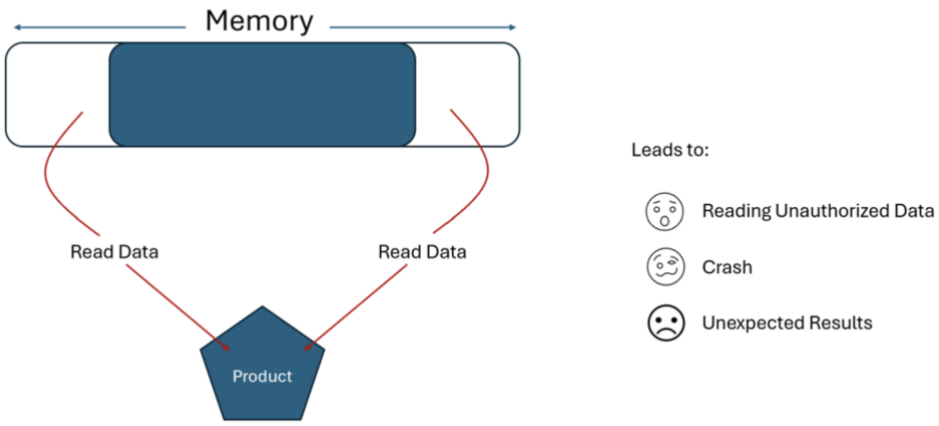

Figure 37: *Screenshot from VisionSpace Group article of the Out-of-Bounds read diagram.*

Supply Chain

Supply chains remain a prime target for threat actors, and the space sector is no exception to this growing risk.

China's rapid emergence as a global leader in aerospace and defence manufacturing underscores a significant vulnerability. From 2005 to 2020, the number of Chinese suppliers embedded in U.S. defence supply chains quadrupled. Moreover, between 2014 and 2022, U.S. reliance on Chinese electronics surged by 600%. This escalating dependence has raised serious concerns about the potential risks associated with relying on China's industrial base, including the possibility of vulnerabilities being intentionally or inadvertently introduced into critical U.S. systems.

Figure 38: *Graphic illustrating the rise of Chinese suppliers in U.S. defence supply chains.*

The U.S. industrial base is currently facing challenges in scaling aerospace and defence production, particularly amid the ongoing Ukraine conflict. As a result, the U.S. has become increasingly reliant on adversarial states, including China, for the manufacturing of critical weapon systems. This dependency is especially pronounced for certain air-launched systems, which often integrate technologies applicable to space systems.

Prominent defence contractors appear to be deeply embedded in supply chains that originate in China, playing a pivotal role in advancing U.S. space ambitions. However, this integration brings inherent risks. It is highly likely that these defence primes are already susceptible to supply chain compromises, particularly through overseas-sourced components critical to their operations.

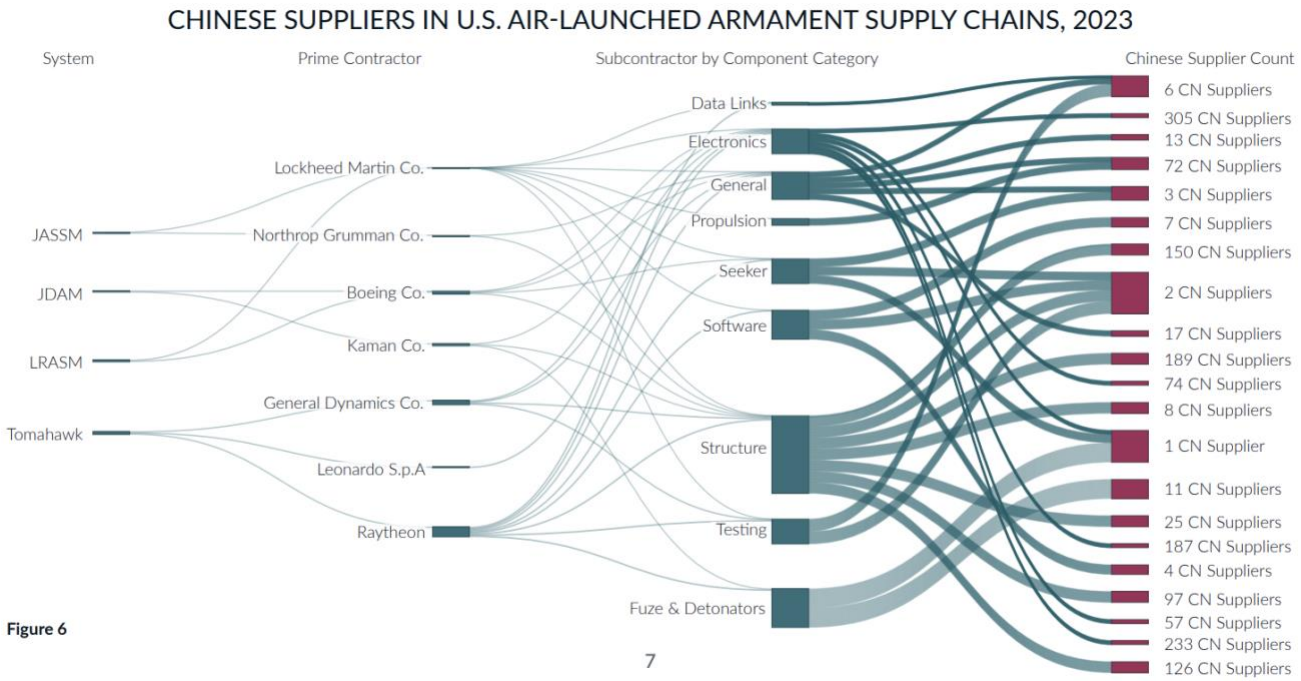

Figure 39: *Graphic illustrating the presence of Chinese suppliers in air-launched armament supply chains.*

One of the most notorious examples of cross-sector cyberattacks, including its impact on the aerospace sector, was the SolarWinds hack of 2020. Widely attributed to the Russian intelligence agency (SVR) and its associated threat actor BlueBravo (also known as APT29 or Cozy Bear), the attack exploited SolarWinds' Orion software. The attackers injected malicious code, later dubbed “Sunburst,” into a legitimate software update. When customers unknowingly downloaded and installed the compromised update, they granted the attackers unauthorised access to their systems.

This breach affected numerous aerospace and defence contractors, providing the attackers months of undetected access. During this time, they were able to steal sensitive data, monitor internal communications, and potentially implant additional backdoors for future exploitation.

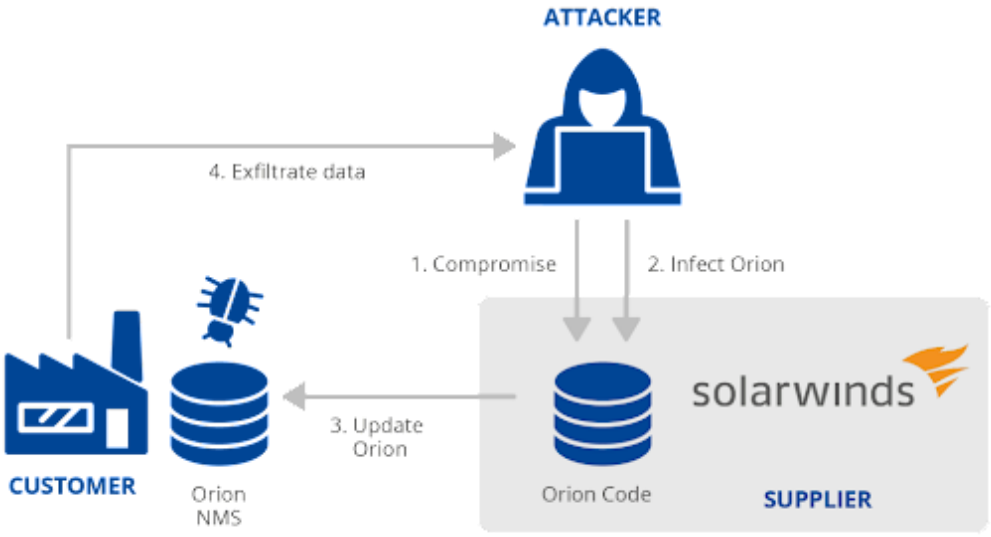

Figure 40: *High-level depiction of the SolarWinds compromise from ENISA.*

In the same year, the DoppelPaymer ransomware group targeted Digital Management Inc. (DMI), a NASA contractor. DMI provides critical IT services to NASA, including support for its space missions and other essential operations. DoppelPaymer claimed to have exfiltrated a substantial volume of sensitive files containing proprietary information, contracts, and other details related to NASA's activities.

To pressure DMI into paying the ransom, DoppelPaymer published portions of the stolen data on their dark web leak site, showcasing their access and amplifying the intimidation. Neither NASA nor DMI publicly disclosed whether a ransom was paid or the full extent of the compromised information.

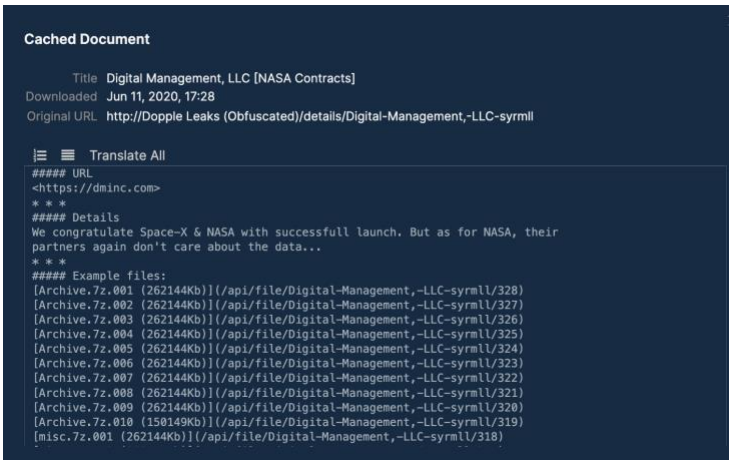

Figure 41: *Cached post in the Recorded Future Intelligence Cloud from Dopple Leaks featuring download links (.zip and .7z formats) allegedly containing sensitive information about NASA operations and projects, as claimed by DoppelPaymer.*

In 2023, the LockBit ransomware gang launched an attack against Maximum Industries, a Texas-based manufacturing contractor that provides services to SpaceX. LockBit claimed to have stolen sensitive data related to SpaceX, including files purportedly containing information about the company's spacecraft and equipment.

The group published a ransom note on their dark web leak site, asserting that they had obtained "3,000 drawings certified by SpaceX engineers" and threatening to auction the stolen data to the highest bidder. Despite the bold claims, neither SpaceX nor Maximum Industries publicly commented on the incident, including whether a ransom was paid or the extent of the breach.

Mitigations

Threat Landscape Analysis: Regularly monitor and stay informed about the latest cyber security threats and developments in the space sector. This can be done by subscribing to reputable sources, ingesting finished intelligence on the threat landscape, attending related conferences such as CYSAT, and participating in industry forums.

Figure 42: *Defence Space 24 was hosted in London at the end of September 2024. Government, military and industry representatives attended the event.*

Vulnerability Assessment: Identify potential vulnerabilities in both ground-based and space-based systems, including communication links, satellite control systems, and data transmission pathways. Organisations should maintain an intelligence-led patch management process to ensure assets are up to date with the latest security patches. This helps protect against known vulnerabilities that cyber attackers may exploit.

Encryption and Secure Communication: Ensure that all data transmitted to and from space assets (satellites, spacecraft, etc.) is encrypted using robust encryption protocols to prevent interception or tampering. Employ MFA to access satellite control systems, mission-critical ground stations, and other sensitive infrastructure to minimise unauthorised access.

Supplier Vetting and Auditing: Ensure that components and software used in space systems, especially those deemed critical, are sourced from trusted and secure suppliers. Regularly audit suppliers for adherence to cybersecurity

standards and ensure that contracts include clauses that address cybersecurity responsibilities and liabilities specific to space systems. Furthermore, review the risk your supply chain faces from cyber attacks, e.g. do they have lots of exposed credentials? Do they have vulnerabilities that can be publicly identified and exploited? Define actions to take which address your high-risk suppliers.

Government and Industry Partnerships: Engage in partnerships with governmental space agencies, aerospace organisations, and industry groups to share threat intelligence and best practices. Establish tested protocols for reporting cyber incidents related to space assets and coordinate with relevant authorities to mitigate potential impacts.

Outlook

As the race to dominate space accelerates, it is almost certain that cyberattacks targeting space-related organisations and technologies will also accelerate.

This white paper has examined the evolving stages of the space race, confirming that competition for Earth's orbit is well underway. The rivalry between U.S.- and Chinese-led lunar colonisation efforts continues to escalate. Meanwhile, companies are racing to develop technologies for asteroid mining, and planetary exploration is poised to lead to the establishment of human presence on distant planets and moons.

In response to this accelerating competition, nations are heavily investing in their national space missions and private-sector partnerships to gain an edge. Militaries are reorganising to integrate cyber and space capabilities, as seen with the creation of the U.S. Space Force and the PLA Aerospace Force. It is highly likely that other nations will follow suit by establishing or expanding their own space commands and defence forces.

Since the late 2010s, cyberattacks targeting the space sector have increased dramatically, particularly against ground stations. This trend underscores why space operations are increasingly collaborating with cyber units, as explored in this paper using the U.S. and China as key examples. Espionage-related cyber threats aimed at providing nations with technological superiority in space are nearly certain to intensify. Signal hijacking is likely to continue disrupting space operations, intercepting sensitive information, or spreading propaganda. Destructive cyberattacks targeting ground stations or damaging orbital assets are also likely to become more frequent. Moreover, supply chain attacks against the space sector are nearly certain to increase significantly, posing risks to critical components and technologies.

To address these challenges, organisations operating in the space domain must remain vigilant against cyber threats. It is crucial for these entities to strengthen their defences by addressing vulnerabilities, implementing robust encryption protocols, securing supply chains, and fostering industry partnerships to share intelligence and best practices.

Ultimately, the stakes are monumental. Whoever dominates cyberspace will dominate outer space, and whoever dominates outer space will shape the trajectory of humanity's future beyond this world.

Appendix A

Description	Link to Advanced Query
Aerospace & Insikt Research Leads	Link
Spaceport Launch References	Link
United States Space Force Mainstream News or Analyst Notes	Link

***Appendix Table 1**: Advanced queries in the Recorded Future Intelligence Cloud.*

Appendix B

ICARUS Matrix: generating novel scenarios in outer space cybersecurity

***Instructions**: Pick a variable from two or more columns to construct a scenario. This is not a comprehensive list but only a starter kit.*

	A: Threat actors	B: Motivations	C: Cyberattack methods	D: Victims / stakeholders	E: Space capabilities affected
1	Major space-faring states	Nationalism	Insider attack	Major space-faring states	GPS / GNSS
2	Other space-faring states	Dominance / influence	Social engineering	Other space-faring states	Earth observation / remote sensing
3	Non-space-faring states	Financial / economic	Ransomware	Non-space-faring states	Military intelligence and capabilities
4	Insider threats	Fraud	Honeypot	State-owned entities	Spacecraft, robotic or crewed
5	Political terrorists	Employment	Sensor attack	Military and other contractors	Life-sustaining services
6	Mercenaries	Blackmail / coercion	Signals jamming	Scientific organizations	Other essential services
7	Eco-terrorists	Terror	Signals spoofing or hijacking	Corporations	Other safety of personnel / others
8	Corporations	Warfare	Eavesdrop / man-in-the-middle	Wealthy individuals	Loss of sovereignty / control
9	Mobile service providers	Disinformation	Network security	General population / society	Earthbound services
10	Launch service providers	Espionage	Supply chain, hardware	Indirect / secondary stakeholders	Emergency services
11	Social engineering groups	Sabotage	Supply chain, software	Marginalized populations	Financial transactions
12	Organized crime	Extremist ideology	AI / ML / computer vision	Social movements	Mining or manufacturing
13	Chaos agents	Cult of personality	Attack coverup	Cultural / religious groups	Scientific capability / research
14	Religious / apocalyptic	Paranoia / anti-technology	Software hacking	Unions / labor reps	Asteroid detection systems
15	Other ideological groups	Boredom / trolling	Systems security	Customers / users via their data	Space weather monitoring
16	Proxies / agents, esp. unwilling	See world burn / chaos	Multi-phase attack / APT	Individual targets	Space traffic management
17	Noncombatants, esp. unwilling	Social / distributive justice	Cloud hacking	Critical specialists	Space tourism
18	Amateur hackers / enthusiasts	Intellectual / tech demo	Account compromise	Critical infrastructure	Launch capabilities
19	AI / machine learning	Revenge / retaliation	Quantum computing / comms	Internet / media / entertainment	Communications
20	Unknown / anonymous	First contact, for and against	Death by 1,000 cuts / long game	AI / machine learning	News / social media

Version 1.0 © Ethics + Emerging Sciences Group at Cal Poly, 2024 Full report: https://spacecybersecurity.org

***Appendix Table 2**: Summary of the ICARUS Matrix from https://ethics.calpoly.edu/spacecyber.html*

Note: Recorded Future AI was used to research topics covered in this paper and to refine sections of this paper

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Recorded Future

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,900 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence. Learn more at recordedfuture.com.