2

THE THREAT LANDSCAPE

This chapter provides a comprehensive overview of space-specific threats, highlighting how adversaries can disrupt spacecraft operations through electromagnetic interference or by physically damaging satellites. We will also explore how traditional cyber threats such as malware, unauthorized access, and data breaches can manifest in the context of space missions.

Adversarial threats to space systems are intentional and often highly sophisticated. These threats come from nation-states, criminal groups, insiders, and other actors aiming to disrupt, degrade, or exploit space-based assets. Unlike random failures or environmental hazards, adversarial threats are strategic, targeted, and constantly evolving. These aren't the only dangers to space systems, however; we'll also discuss the risks posed by nonadversarial threats, including natural hazards such as radiation, space weather, micrometeoroids, and space debris.

Anti-Satellite Weapons

Anti-satellite weapons (ASATs) are military systems designed to disable, destroy, or impair satellites critical for communication, navigation, intelligence, and military operations. The proliferation of ASAT technologies has raised concerns about an arms race in space and its implications for the international security order.

We can broadly categorize ASAT systems as either kinetic or non-kinetic. *Kinetic* ASATs are designed to physically destroy or incapacitate a target satellite through direct impact. These systems typically use missiles, projectiles, or even co-orbital spacecraft to collide with the target, causing it to break apart or become inoperable.

Non-kinetic ASATs, on the other hand, rely on alternative means to disrupt, damage, or disable spacecraft. For example, they may use directed-energy weapons (such as lasers), signal interference techniques (such as jamming or spoofing), or co-orbital satellites to interfere with spacecraft operations. Non-kinetic approaches generally leave the satellite physically intact but can render it useless by disrupting its functions or communications.

We'll focus on kinetic weapons in this section and consider non-kinetic approaches in "Electronic Warfare" on page 19. We'll also look at other potential physical attack vectors, before turning our attention to more traditional cyber warfare techniques.

Direct Ascent

Rockets, the most commonly used type of kinetic ASAT, are designed to intercept and destroy satellites in orbit. These are often referred to as direct-ascent ASATs because they are launched from the ground or from fighter jets and travel directly to intercept their target without first entering orbit. A rocket's boost stage accelerates it to high enough relative velocities that it can destroy a satellite upon impact, without the need for explosives.

To validate the effectiveness of kinetic systems or demonstrate their military capabilities, nations have conducted ASAT tests that target their own satellites. As those tests have shown, these actions often generate large amounts of space debris. For example:

- In 1985, the United States demonstrated its air-launched ASM-135 ASAT by destroying a defunct research satellite flying at an altitude of 555 km. Nearly 300 pieces of debris were generated, with the last one remaining in orbit for almost 20 years.
- In 2007, China destroyed an old weather satellite at an altitude of 865 km using a kinetic kill vehicle, resulting in the largest debris field in history. Many of the over 3,000 trackable pieces of debris are expected to remain in orbit for decades or centuries.
- In 2019, India's Mission Shakti used a kinetic kill vehicle to destroy a satellite that had been launched for the purposes of the test at a low altitude, to minimize long-lasting debris.

- In 2021, Russia used a direct-ascent missile to destroy a defunct satellite at an altitude of about 480 km, creating 1,500 pieces of debris that still endanger the ISS.

Efforts to ban such tests have been proposed but face challenges due to geopolitical dynamics.

Co-Orbital

Unlike direct-ascent ASATs, co-orbital weapons enter orbit and then maneuver to approach their target and disable, damage, or destroy it. These weapons pose a serious threat due to their ability to remain dormant in orbit until activated, allowing for stealthy and unpredictable attacks.

Co-orbital ASATs can use a few different attack methods. Direct collision weapons deliberately collide with their target at high velocities, while others release high-speed fragments or shrapnel to increase the likelihood of a collision. Certain systems employ robotic arms to physically manipulate, damage, or remove satellite components. At close range, some may use electronic and cyber warfare techniques or directed-energy weapons, as discussed in the following section, to disrupt satellite functions.

Although the Outer Space Treaty prohibits nuclear weapons in orbit, high-altitude nuclear detonations were tested during the Cold War. More recently, in its 2025 Annual Threat Assessment, the US intelligence community accused Russia of potentially deploying a nuclear weapon in orbit.

While co-orbital ASAT technologies may have peaceful applications, such as satellite servicing, inspection, and debris removal, concerns have grown about their potential as weapons. The ability to position and activate them covertly introduces a new dimension of strategic uncertainty in space operations. Furthermore, they pose a significant risk of generating long-lasting orbital debris, exacerbated by the growing congestion in key satellite orbits. The continued development and potential deployment of these systems remains a critical issue in international space security discussions, and efforts are being made to establish norms and treaties to mitigate their risks.

Electronic Warfare

Electronic warfare comprises any adversary action that uses electromagnetic energy to achieve specific objectives, such as jamming, spoofing, or various types of directed-energy attacks. Its aim is typically to deny adversaries effective use of the electromagnetic spectrum while ensuring that friendly forces can continue to use it.

Jamming

A jamming attack overwhelms signal receivers with intense electromagnetic noise by transmitting strong signals in the target system's frequency range.

To target static-frequency systems, adversaries use *spot jamming*, which focuses on a narrow frequency band to block a signal. They may also target

broadband signals with *sweep jamming*, moving the signal across the target bandwidth, or use *barrage jamming* to target multiple frequencies simultaneously by distributing power across the target ranges.

Another technique, *pulse jamming*, where short bursts of noise block or mask specific areas, can disrupt radar systems. For instance, jamming attacks have targeted *synthetic aperture radar (SAR)* satellites, which use radar signals instead of light to generate high-resolution images. Figure 2-1 is an example of harmful interference recorded by one SAR satellite, ESA's Copernicus Sentinel-1.

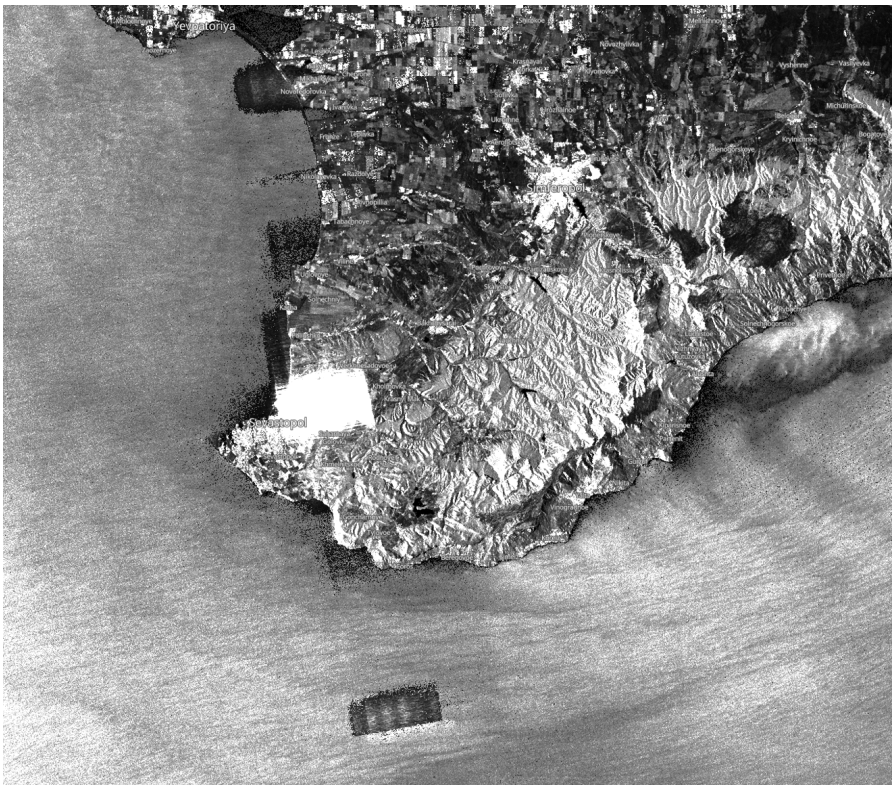

Figure 2-1: SAR interference over Sevastopol, in Crimea, Ukraine

Although SAR images don't capture visible light, color is often added during post-processing to make the data easier to interpret. Areas that reflect stronger radar signals might appear in bright colors, while regions with weaker reflections might appear darker.

The bright feature near the center of this image, captured in November 2023, isn't a natural part of the landscape but an artifact caused by signal interference that disrupted the Copernicus Sentinel's ability to create an image of the territory.

Spoofing

Interference isn't always about blocking signals. Some attacks aim to deceive systems entirely, which brings us to spoofing. Spoofing is a deception technique that involves transmitting false signals to trick other systems into perceiving incorrect information, causing them to make misinterpretations and errors.

Attackers may combine spoofing and jamming to increase the effectiveness of their interference. A commonly used technique is to block all frequency bands of the GNSS spectrum except the one on which a spoofed signal is transmitted; the counterfeit signal might then lead the receiver to compute incorrect position or timing data. Similarly, a burst of jamming can cause receivers to lose synchronization, making a connection to a spoofing source more likely once the jamming stops.

In military applications, the increased use of drones on the battlefield has led to a dramatic increase in spoofing. Many highly sophisticated spoofing attacks have targeted radars to create the appearance of nonexistent objects or manipulate signals for real objects.

High-Power Microwave Weapons

High-power microwave weapons are a type of directed-energy technology that emits intense bursts of electromagnetic energy in the microwave frequency range (300 MHz to 300 GHz). They're designed to disrupt, degrade, or destroy electronic systems by overloading circuits and inducing currents, which can permanently damage components such as chips and printed circuit boards.

Because the effective range of these weapons is generally limited to no more than a few kilometers, they can affect airborne targets such as drones, but their large power requirements make them ineffective against satellites when deployed from Earth.

High-power microwave weapons operate in either *pulsed wave mode*, to deliver short bursts, or *continuous wave mode*, for continuous denial of operations. *Narrow-band* devices focus energy on a small frequency range, offering better transmission characteristics, but are limited to specific targets. *Wide-band* devices cover a broad frequency range, enabling more diverse targets with unknown absorption characteristics.

In space warfare, microwave weapons have several advantages: They don't cause debris, they're more challenging to locate than rockets, and they can target multiple objects simultaneously. Satellites can be equipped with directed-energy payloads, although again, their high power demands limit their effective range.

High-Energy Lasers

Another type of directed-energy weapon system, high-energy lasers focus a beam of light to deliver large amounts of energy to a target. These lasers

typically operate in the infrared spectrum and can damage targets by heating them, vaporizing their coatings, or harming sensitive electronics.

There are multiple types of lasers. Solid-state lasers use crystals as a medium. Fiber lasers, which use optical fibers, are more compact and efficient. Gas lasers excite gases, such as CO_2, to emit photons.

Lasers emerged as an ASAT due to their ability to disrupt or destroy satellites with a low risk of creating space debris. One notable attack they can perform is *sensor dazzling*, which blinds optical satellite sensors by overwhelming them with intense light input. This is especially effective against imaging and surveillance satellites that operate in the visible or infrared spectrum.

Higher power levels can cause permanent damage to sensors or optical components such as lenses and mirrors, or even lead to structural damage and debris. Theoretically, a laser could someday impart small forces on satellites to alter or de-orbit them, but due to the vast power required for such an attack, this remains speculative today.

Electromagnetic Pulses

An electromagnetic pulse (EMP) is a burst of electromagnetic energy that can disrupt or damage electronic systems. EMPs originate from natural phenomena such as solar storms and lightning, as well as artificial sources such as nuclear detonations or specialized microwave weapons. The pulse typically rises to peak intensity within nanoseconds and rapidly decays, covering a wide range of frequencies.

Unshielded devices are especially susceptible to EMPs, as they can introduce high voltages and currents in electronic components. Coupling effects, where electromagnetic energy interacts with antennas or conductive materials, amplify the damage.

In space systems, EMPs are effective due to the lack of atmospheric shielding, but in military systems, layered shielding and redundancy can help protect against them.

Other Physical Attack Vectors

In addition to direct attacks on spacecraft, space systems can be disrupted through physical attacks targeting supporting infrastructure on Earth. These include ground-based facilities and communication links that satellites depend on for operation and data transmission. Although indirect, these attacks can have serious consequences, affecting not only individual systems but also broader network functionality.

Ground Segment Attacks

Threat actors may target the ground segments of space systems. For example, intruders could attempt to gain unauthorized physical access to ground station facilities, then damage equipment or steal sensitive data. Insiders,

disgruntled employees, or contractors with access to sensitive systems could also cause security breaches.

To mitigate these physical threats, spacecraft operators typically implement security measures such as perimeter fencing, surveillance cameras, and security personnel, supported by regular risk assessments and disaster recovery planning.

Undersea Cable Damage

Undersea communication cables form the backbone of global telecommunications networks, and damage to these cables can have major implications for satellite operations.

When undersea cables fail, affected regions often use satellite networks to maintain connectivity. The resulting surge in demand places pressure on those networks, which must suddenly accommodate a much larger volume of data than usual. Cables may transmit terabytes of data per second, but most commercial satellite services are considerably slower. So, while satellites can serve as an emergency solution, they can't fully replace the extensive data transmission capabilities of fiber-optic cables.

Satellites that rely on ground stations in remote locations, such as the High North, are more dependent on undersea cables and therefore more vulnerable to attacks on this infrastructure. This creates a dilemma when other services depend on them as a backup.

Although most undersea cable disruptions have resulted from natural disasters and accidents, recent incidents highlight a growing trend of intentional sabotage as part of hybrid warfare strategies. Russia and China have increasingly targeted underwater sea cables, particularly in the Baltic Sea and around Taiwan. Russia has also deployed a "shadow fleet" of vessels to conduct hybrid warfare against NATO, including by damaging European undersea cables. These operations are often performed under the guise of commercial activity, making attribution and accountability difficult.

Cyberattacks

As space systems become increasingly important, cybersecurity vulnerabilities have emerged as critical concerns. These systems' unique characteristics, such as remote accessibility, reliance on extensive data systems, and integration of commercial, off-the-shelf components, make them particularly susceptible to cyberattacks.

While spacecraft computers might previously have had unique architectures, most new systems have an embedded Linux component onboard. Further, the ground segment is often distributed across several sites, as in most modern corporate networks. Factor in the use of cloud resources for good measure, and soon you will realize that the mantra "complexity is the enemy of security" is just as true for space systems as it is for typical IT infrastructure.

In this section, we highlight the cyber threats we see as especially relevant to space systems, including some you'll encounter in typical IT systems

and some you might know from working in OT environments. Subsequent chapters will dive into sophisticated cyberattacks on the ground, space, and user segments, but you can prevent most common attacks with good cyber hygiene implemented across the organization.

Hijacking

Hijacking occurs when threat actors take unauthorized control of a computer system, network, communications system, or spacecraft. In space systems, attackers have exploited vulnerabilities in ground stations, insecure communication protocols, or weaknesses in onboard systems to gain control.

For example, in 2007 and 2008, attackers hacked two NASA satellites, Landsat-7 and Terra AM-1, and took control of them for several minutes. More recently, in cybersecurity demonstrations, ethical hackers successfully hijacked operational satellites by injecting malicious code into the onboard flight software, allowing them to manipulate controls.

Many hijacking attacks target ground stations, which often use insecure protocols and may lack strong security measures. Once compromised, attackers can sometimes use their access to send unauthorized commands to a spacecraft.

Phishing

In a phishing attack, threat actors impersonate trusted entities to steal sensitive data or deliver malware through deceptive communications such as emails, text messages, or phone calls. The goal is usually to get victims to click malicious links, share sensitive credentials, or transfer funds.

Phishing is a serious risk to satellite missions because if attackers can exploit human error, they can compromise ground control systems in numerous ways. For example, once they've stolen credentials or deployed malware, they may be able to send unauthorized commands, interfere with operations, manipulate telemetry, or exfiltrate sensitive mission data.

Phishing simulations and awareness training can help reduce the likelihood of someone opening a PDF or clicking a link, but the risk is unlikely to disappear entirely.

Distributed Denial of Service

A distributed denial-of-service (DDoS) attack is a cyberattack designed to overwhelm a target server, website, or network with traffic, rendering it inaccessible for legitimate users. Unlike standard denial-of-service (DoS) attacks, which originate from a single source, DDoS attacks either crowdsource resources or leverage a network of compromised devices, called a *botnet*, to generate traffic from multiple locations simultaneously.

DDoS attacks are especially popular among hacktivist groups, and public-facing space data systems have seen increased targeting since Russia invaded Ukraine. In particular, hacktivists have conducted numerous attacks on the

ground infrastructure supporting Russia's satellite networks. These attacks demonstrated that, although space systems historically have not depended on public-facing websites for critical functions, their growing integration with terrestrial networks and cloud-managed ground stations has expanded their attack surface.

DDoS attacks are relatively easy to implement but have limited impact, as the system becomes reachable again once the attack is stopped.

Zero-Days

Zero-day vulnerabilities are previously unknown security flaws in software and hardware. The term zero-day reflects the fact that vendors have had zero days to address the issue before malicious actors discover it, at which point they may take advantage of it with a zero-day exploit.

Zero-day attacks often target widely used systems or high-value targets such as governmental agencies or critical infrastructure. Attackers try to remain undetected when carrying out these attacks, as the window for exploiting zero-day vulnerabilities closes as soon as they are discovered and patched. State-sponsored actors might also purchase and save these vulnerabilities for high-profile attacks.

Router firmware, firewalls, virtual private network (VPN) gateways, and operating systems (OSes) like Windows and Android are common targets for researchers trying to profit from finding and selling vulnerabilities. However, any software or hardware can have zero-days, especially systems that haven't undergone security testing.

The space sector is highly susceptible to this type of threat, as it runs on standard IT infrastructure with potentially vulnerable components. Furthermore, many spacecraft and satellite systems rely on legacy hardware and software components that are often past their end of life. These outdated systems may no longer receive security updates or patches, exposing them to exploits once a zero-day is discovered. The difficulty of physically accessing or updating satellites in orbit amplifies the potential impact of these attacks.

Later in this book, you'll have several opportunities to find and exploit a zero-day vulnerability in a space system yourself. We'll start diving into security testing in Chapter 3.

Malware

Malicious software, or malware for short, is any software intentionally designed to harm devices, networks, or data. The name is an umbrella term for a wide range of hostile software that invades systems, corrupts functionality and data, or enables unauthorized access. This includes:

Viruses Attach to legitimate files and corrupt systems. Require user interaction to run and spread. A special subtype, *polymorphic viruses*, change their code and signature to evade simple hash-based detection.

Worms Exploit network vulnerabilities to self-replicate. Unpatched vulnerabilities that allow worms to spread can have large-scale global impacts.

Trojans Disguise themselves as legitimate software to create backdoors, enabling further exploitation and lateral moves across an organization. Trojans can be delivered in a phishing campaign and become the entry point for future attacks.

Spyware Monitors user activity to steal data, such as credentials and secret files. Keyloggers, for example, record keystrokes to capture passwords or financial data such as credit card numbers. In high-profile attacks, actors employ sophisticated techniques to avoid the detection of exfiltrated data and enable long-term persistence in targeted systems.

Rootkits Conceal malicious software activity to avoid detection by antivirus software and operating system protections. They can be used to support or embed other types of malware. Attackers can purchase rootkits that leverage unpatched weaknesses, while more advanced actors might create custom kits to enable their operations.

Botnets Infect devices and turn them into remotely controlled, centrally orchestrated attack tools used to spread further malware or perform DDoS attacks. Botnet software often targets outdated web servers or vulnerable internet of things (IoT) devices.

Ransomware Encrypts files to extort money. The most prevalent malware, ransomware often demands payment in cryptocurrencies such as Bitcoin or Monero. Payment usually doesn't guarantee that the data can be recovered. Sophisticated attackers may also exfiltrate sensitive files and threaten to sell or leak them. Darknet vendors have created ransomware-as-a-service kits that allow criminal organizations without in-depth technical know-how to conduct attacks at scale.

Advanced attackers can assemble these into highly specialized and targeted cyber weapons. The case of Stuxnet, discussed in the following box, exemplifies how precisely designed malware can cause physical disruption to critical infrastructure. It also demonstrates the potential of advanced threats to exploit technical vulnerabilities and operational assumptions, such as the security of airgapped systems.

STUXNET: HOW MALWARE CAN SABOTAGE INFRASTRUCTURE

Stuxnet was a computer worm designed to target programmable logic controllers (PLC) used in supervisory control and data acquisition (SCADA) environments. Developed under the US–Israel joint operation *Olympic Games*, Stuxnet was meticulously engineered to sabotage Iran's nuclear program.

Because Iran's nuclear facilities were isolated from the internet, the attackers introduced Stuxnet via infected USB drives carried into the facilities, likely by insiders or agents. Once inside, it propagated and executed autonomously across networked systems using four zero-day vulnerabilities. Stuxnet delayed Iran's nuclear program by months to years, though no state officially claimed responsibility.

The Stuxnet worm was the first recorded case of a sophisticated cyber weapon used in the wild, and it demonstrated the viability of cyber weapons for physical infrastructure sabotage. Further, it demonstrated that airgapped networks are only effective if operators take measures to ensure they remain safe.

Supply Chain Attacks

Supply chain attacks aim to infiltrate systems by targeting the third-party components they employ. By breaching a vendor, contractor, or software dependency with weak security or a small contribution base, an attacker can affect many downstream organizations and systems.

A striking example of a modern software supply chain attack is the 2024 compromise of XZ Utils, a core library embedded in countless Linux distributions. This attack unfolded gradually, revealing how even widely trusted software can become a vector for deep system compromise when its stewardship is subverted.

Over the course of multiple years, the attacker embedded a malicious backdoor into the widely used open source compression library *xz/liblzma*. The attack targeted Linux distributions by compromising SSH authentication through a compromised dependency.

This attack made use of significant social engineering. The attacker gained maintainer status for XZ Utils after a prolonged campaign. Fake accounts pressured the original maintainer to relinquish control, citing burnout and inactivity. The attacker contributed legitimate code for nearly two years before introducing the backdoor in 2024, evading detection through gradual, trusted contributions.

While the attack's discovery by a developer in 2024 prevented its widespread exploitation, the incident highlighted vulnerabilities in open source maintenance and supply chain trust. Affected systems included bleeding-edge Linux distributions such as Fedora Rawhide and Debian testing/unstable versions. The identity of the threat actor remains unknown, but the complexity of the operation suggests state-sponsored participation.

Modern space systems rely heavily on Linux, including for a spacecraft's onboard computers. Supply chain attacks that affect embedded Linux systems often target libraries or utilities critical to system functionality. Embedded systems frequently integrate open source libraries with minimal oversight, and devices may lack automated patching, exposing them to unaddressed vulnerabilities.

Case Study: The APT Attack of the KA-SAT Satellite Network

Several of the examples we've discussed so far, such as Stuxnet, were the work of *advanced persistent threats (APTs)*: sophisticated, well-resourced threat actors, often sponsored by states or organized crime groups. APTs commonly target critical infrastructure by leveraging stealth and sophisticated tactics to inflict long-term damage, so they pose a substantial risk to the security of space systems.

One real-world example of an APT targeting satellite communication infrastructure occurred in early 2022, when a cyberattack on Viasat's KA-SAT satellite network coincided with the onset of Russia's invasion of Ukraine. This attack disrupted military communications and highlighted the vulnerabilities in satellite systems, underlining the growing threats to space-based technologies.

On February 23, 2022, the attackers exploited a VPN appliance in a management center in Turin, Italy, accessing servers controlling modem software updates. They deployed AcidRain, a dedicated wiper malware that erased critical data on modems, rendering them inoperable. Restoring them was only possible using a physical debugging interface. In a secondary attack, the attackers overwhelmed Viasat's servers with a custom DoS attack tailored to the internal management network, preventing more modems from connecting.

The European Union, United States, and United Kingdom formally blamed Russia, citing ties to the GRU-linked Sandworm APT group. The attack peaked on February 24, when it disrupted communications for Ukrainian military operations and, as collateral damage, caused 5,800 wind turbines in Germany to become unreachable. It severely hindered Ukrainian military capabilities during the critical early hours of the invasion. Viasat stabilized its network within a few days but faced ongoing attacks.

Today, the incident is considered one of the most disruptive operations in the history of cyber warfare and underscores the serious consequences of cyberattacks on space systems. We'll explore the attack in depth in Chapter 10.

Nonadversarial Threats

Not all threats to space operations come from hostile actions or deliberate interference. As you learned in Chapter 1, many risks arise from natural and environmental factors. This section explores these nonadversarial threats, including radiation, space weather, extreme temperatures, vacuum conditions, atmospheric effects, micrometeoroids, and space debris.

Radiation

Radiation is energy transmitted through a material or free space in the form of waves or particles. Electromagnetic radiation includes radio waves, infrared radiation, visible light, ultraviolet radiation, X-rays, and gamma radiation, while particle radiation consists of alpha, beta, proton, and neutron particles.

Another way of classifying radiation is as ionizing and non-ionizing. *Ionizing radiation* carries more than 10 electron volts (eV) of energy and can ionize molecules and break chemical bonds. *Non-ionizing radiation* lacks enough energy to cause ionization; it includes electric fields, magnetic fields, and optical radiation.

In space, there are three primary sources of radiation: galactic cosmic rays, solar energetic particles, and trapped radiation. Cosmic rays are high-energy particles that originate outside the solar system. They can arise from cosmic events such as supernovae and mainly consist of protons and alpha particles. Particles from our sun include protons and heavier ions emitted during solar flares and coronal mass ejections. These particles can reach very high speeds and present a serious risk to astronauts and spacecraft. Lastly, spacecraft and astronauts may be affected by charged particles trapped by Earth's magnetic field.

Our planet is surrounded by two doughnut-shaped regions of intense radiation called the *Van Allen belts*, formed by the interaction between the solar wind (see "Solar Wind" on page 31) and Earth's magnetic field. The belts consist of multiple dynamic layers of trapped particles, including high-energy electrons and protons. They can pose hazards to both satellites and astronauts due to the high levels of energetic particles they contain.

Damage to Electronics

Ionizing radiation in space can have a significant effect on a spacecraft's electronics and materials. Long-term exposure can damage electronic components, leading to threshold voltage shifts, increased leakage currents, and reduced performance or failure of semiconductors. As a result, solar cells experience substantial performance degradation over time.

Closely related to radiation exposure is the phenomenon of *dielectric charging*, which occurs when radiation interacts with dielectric materials, causing the accumulation of electric charge within them. Dielectric materials are electrical insulators that don't conduct current but can store electric fields through polarization, in which an external electric field causes charges within the material to shift.

In addition to these long-term effects, radiation can cause *single-event effects (SEEs)*, which are temporary or permanent disruptions in electronic systems triggered by a high-energy particle hitting a sensitive region of a microelectronic device. Beyond bit flips in memory, SEEs can induce undesired processor behavior such as unexpected resets, logic errors, or disruptions in command flow, potentially leading to mission-critical failures. Other examples include latch-ups, where a short-circuit is created within a semiconductor, and burnouts, where components are permanently damaged.

SEEs are particularly significant for modern spacecraft, which rely on high-density, small-feature electronics. Mitigation techniques such as error-correcting codes, redundant systems, and radiation-hardened components can help maintain their reliability.

Other Effects

Radiation can degrade materials other than electronics. It can weaken spacecraft materials by causing discoloration or molecular changes, making them brittle. Mission planners can mitigate these effects through shielding or by reducing the time spent in high-radiation zones like the Van Allen belts.

Radiation can also interact with spacecraft materials to produce lower-energy, secondary radiation, adding to the risk posed to both electronics and human occupants.

Space Weather

In space, weather phenomena driven by the sun can interact with Earth's magnetic field and atmosphere in ways that impact both space and ground systems, causing disruptions in radio communication links and power grids and damage to electronic devices.

Agencies such as NASA, NOAA, and ESA continuously monitor the sun to measure and predict space weather conditions. You can find up-to-date information on current weather conditions in space on the websites of the NOAA Space Weather Prediction Center (*https://www.swpc.noaa.gov*) and the ESA Space Weather Network (*https://swe.ssa.esa.int/current-space-weather*).

Sunspots and the Solar Cycle

Two closely related phenomena, sunspots and the solar cycle, occur on the sun's surface and affect its activity. Sunspots are dark, cooler areas of the sun's surface that form in places where the magnetic field is more potent and blocks some heat from reaching the surface. (Of course, even these cooler areas still reach temperatures around 3,600 degrees Celsius, or 6,500 degrees Fahrenheit.) Sunspot activity varies with the solar magnetic cycle, which completes approximately every 11 years. There are the fewest sunspots when the solar cycle reaches its minimum and the most when it reaches its maximum.

Solar Wind

The sun's outermost corona layer continuously releases a stream of charged particles called the solar wind. This plasma stream primarily consists of electrons and protons from hydrogen nuclei, although it is about 10 percent alpha particles and has smaller amounts of heavier ions. Depending on solar conditions, the wind typically reaches speeds ranging from 300 to 750 km/s (about 185 to 465 mi/s). While the particle temperature varies, it can reach up to around 1 million degrees Celsius (1.8 million degrees Fahrenheit).

Although Earth's magnetic field protects us from most of the particles carried by the solar wind, they can enter in greater numbers near the poles. The interaction between these particles and the magnetic field produces auroras, mesmerizing natural light displays characterized by dynamic patterns of brilliant color visible in high-latitude regions. It can also trigger other space weather phenomena, such as geomagnetic storms and radio blackouts.

Solar Flares

Solar flares are powerful bursts of electromagnetic radiation that typically originate in regions of intense magnetic activity around sunspots. They are among the most energetic events in the solar system and can have a considerable impact on the space environment.

Solar flares occur when twisted magnetic field lines suddenly realign and release stored magnetic energy. These events can last from minutes to hours, depending on the amount of energy released. When energy stored in the magnetic field is released during a flare, it heats solar material to tens of millions of degrees Celsius and causes the emission of radiation across the electromagnetic spectrum, from radio waves to gamma rays.

Scientists classify solar flares based on their X-ray intensity in the 0.1 to 0.8 nanometer (nm) band. The most powerful are X-class flares, capable of causing global radio blackouts and long-lasting radiation storms. M-class flares, of medium intensity, can cause localized disruptions. C-, B-, and A-class flares are progressively weaker events with minimal to no effect on Earth.

Coronal Mass Ejections

Coronal mass ejections (CMEs) are eruptions of large amounts of plasma and magnetic field from the sun's corona. While solar flares and CMEs often occur together, they are distinct phenomena: Whereas solar flares are localized bursts of electromagnetic radiation capable of traveling at the speed of light, CMEs consist of billions of tons of magnetized plasma propelled at lower speeds, typically between 250 km/s and 3,000 km/s.

Without the protection of Earth's magnetic field, astronauts and spacecraft can accumulate high doses of radiation when hit by a CME. In the outer layers of the atmosphere, especially the ionosphere, CMEs can change how signals propagate, causing delays and rapid fluctuations in amplitude and phase. Positioning, navigation, and timing (PNT) systems allow for determining an object's position, guiding its movement, and synchronizing

time-based operations. PNT systems like GPS rely on satellite signals to broadcast information. CMEs lower the accuracy of these systems and can cause blackouts in radio communication, especially between 3 and 30 MHz.

Temperatures

In the previous chapter, we mentioned that extreme temperatures in space can pose a significant risk to spacecraft if not carefully considered and designed for. For example, on the surface of the ISS, materials exposed to direct sunlight can reach temperatures of up to 120 degrees Celsius (248 degrees Fahrenheit), well above the standard rating of many components and materials we use on Earth. By contrast, when in the shade or far from the sun, spacecraft can experience temperatures as low as −150 degrees Celsius (−238 degrees Fahrenheit).

Prolonged exposure to such cold can cause components to fail or materials to become brittle and crack. Moreover, spacecraft often transition quickly between sunlight and shadow, causing rapid thermal cycling. This can further stress materials, leading to failure over time.

It can be challenging to manage temperatures inside and on the surface of a spacecraft because of the lack of convection in space (discussed further in the next section). Before launch, a spacecraft undergoes thermal cycling to ensure that materials are "baked out," meaning that volatile compounds have been removed, and to test the robustness of the thermal control system. To minimize heat transfer and protect components, *multilayer insulation (MLI)* consisting of materials such as Kapton and Mylar is used. Interior temperatures can be stabilized using radiators, which dissipate heat by radiating it into space, and active heaters.

Vacuums

A vacuum is an area devoid of matter. In the context of outer space, the term refers to the nearly empty regions between celestial bodies. These regions contain very few particles and traces of gas, so their pressure is extremely low compared to Earth's atmosphere. In such conditions, materials can release trapped gases in a process called *outgassing*, which may damage or degrade components.

Another challenge related to vacuums is that, in space, convection cannot occur. This makes thermal management more complex, as spacecraft must instead rely on radiative cooling. Without convection, heat cannot be evenly distributed across surfaces, which can lead to localized overheating or cooling, so engineers must carefully consider thermal design to ensure more uniform heat distribution. The absence of convection also complicates the storage and distribution of the liquid propellants that many spacecraft rely on for orbit control thrusters.

On the positive side, without an atmosphere, spacecraft don't experience aerodynamic drag, allowing engineers to design structures that wouldn't function under atmospheric conditions or in stronger gravitational environments.

Atmospheric Effects

Earth's atmosphere comprises five main layers, each with its own characteristics. The *troposphere*, the densest layer, extends from the surface to a height of about 12 km (7.5 miles). Most weather phenomena occur here. Above it is the *stratosphere*, extending to about 50 km (31 miles) and containing the ozone layer, which protects the surface from most harmful ultraviolet radiation. Above this, extending up to about 85 km (53 miles), is the *mesosphere*, the coldest of all layers and the region where most meteors burn up. The *thermosphere* extends from the mesosphere up to between 500 and 1,000 km (about 310 to 620 miles) above Earth's surface and is characterized by increasing temperatures with altitude. The *ionosphere*, a zone of ionized particles extending from roughly 60 km to 1,000 km (37 to 620 miles) or higher, lies mainly within this region; this is where the auroral phenomena described in "Solar Wind" on page 31 occur. Beyond the thermosphere is the *exosphere*, the outermost layer of the atmosphere, which gradually transitions into outer space.

Many satellites operate within the exosphere to lessen the impact of atomic oxygen, which can erode materials such as solar cells through chemical reactions. Oxidation can penetrate more deeply into spacecraft structures than may be expected.

The adverse effects of atmospheric trace gases decrease at higher altitudes. To further mitigate their impact, spacecraft designers must consider protective measures and select appropriate materials for components exposed to the LEO environment. You can find more information about the different orbits and their challenges and use cases in Chapter 1.

Micrometeoroids

Micrometeoroids are tiny particles traveling through space at very high speeds. These particles can cause surface degradation over time, eroding spacecraft exteriors, mirrors, lenses, and sensors. Repeated impacts gradually wear down materials, and even microscopic particles can compromise delicate instruments. Beyond surface wear, micrometeoroid strikes can puncture insulation layers, propellant tanks, pressurized vessels, and essential components such as batteries and coolant lines.

High-velocity impacts can also cause small fragments to break off the spacecraft's surface, potentially altering its attitude or orbit. Even a single impact can cause a loss of precision. Astronauts performing extravehicular activities face additional dangers from micrometeoroids and require specialized spacesuits designed to withstand these impacts, using advanced protective materials such as ceramic-fiber woven barriers and multilayer flexible fabrics.

Space Debris

Space debris consists of human-made objects found in Earth's orbit that no longer serve a purpose, including defunct satellites, abandoned rocket

stages, and mission-related fragments. It is mainly concentrated in LEO, but some also exists in higher orbits. Debris can range in size from tiny paint flakes to large rocket bodies over 10 meters long. When traveling at speeds up to 28,000 km/h, even small pieces of debris can pose a serious threat to operational satellites and spacecraft.

The total mass of all space objects in Earth's orbit exceeds 13,500 tons. Estimates suggest that there are approximately 40,500 objects larger than 10 cm, 1.1 million between 1 cm and 10 cm, and 130 million between 1 mm and 1 cm. The increasing amount of debris has led to concerns about the long-term sustainability of space activities and the potential for a cascade effect when collisions occur.

The *Kessler syndrome* is a theoretical scenario in which the density of objects in LEO becomes so high that collisions between them lead to an exponential increase in space debris. It was proposed by NASA scientists Donald J. Kessler and Burton G. Cour-Palais in 1978. The key idea is that as collisions occur, they generate more debris, thereby increasing the likelihood of future collisions. This risk poses a significant threat to satellites, space stations, and launch activities and could render certain orbital regions unusable for spaceflight.

A critical threshold is reached when new debris is created faster than natural processes remove it. Simulations suggest that the near-Earth environment may already be approaching instability, with debris generation outpacing removal mechanisms such as atmospheric drag. In the final stage of the Kessler syndrome process, referred to as *space congestion*, it is estimated that every satellite in LEO will experience an average of one collision with debris per year. It is unclear when (or if) this will happen, but if space activities continue to increase and orbital space becomes more geopolitically contested, it will likely be only a matter of time before a large-scale cleanup of Earth's orbits becomes necessary.

Now that you have an understanding of the many potential adversarial and nonadversarial threats to space systems, let's quickly review a few of the tools that are available to protect against these hostile actions.

Risk Assessment with the NIST Cybersecurity Framework

As you've learned, the risks to space systems are diverse and complex, ranging from intercepted satellite communications to malicious commands injected into ground station networks. Moreover, assessing risk is particularly challenging in the space domain due to uncertainties associated with environmental factors (such as solar flares) and geopolitical dynamics (such as state-sponsored cyberattacks).

To account for these variables, operators must perform risk assessments that consider both the likelihood of a threat occurring and the potential consequences if it succeeds. Risk management frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 provide structured approaches for this task.

The CSF defines six core functions:

Govern Guides an organization's cybersecurity strategy and oversight, supporting and informing the other five functions.

Identify Involves understanding the organization's assets, risk environment, governance structure, business context, and risk management strategy.

Protect Includes access control, awareness and training, data security, maintenance, and protective technologies to safeguard systems.

Detect Focuses on anomaly and event detection, continuous monitoring, and formal processes to identify incidents promptly.

Respond Encompasses response planning, effective communication, analysis, mitigation actions, and lessons learned.

Recover Emphasizes recovery planning, organizational improvements, and communication to restore operations after an incident.

The CSF also defines four implementation tiers that describe increasing levels of cybersecurity risk management maturity:

Partial Risk awareness is limited and processes may lack consistency.

Risk-Informed Risk awareness begins to inform decision making; risk management practices are approved by management but may not be fully standardized across the organization.

Repeatable The organization has established standardized practices and policies.

Adaptive Continuous improvement is driven by threat intelligence and lessons learned.

Organizations can assess their current tier, set a target tier aligned with strategic objectives, and follow guidance, such as strengthening governance, improving metrics, and embedding feedback loops, to progress over time.

CSF profiles represent an organization's alignment of its risk assessment with its business needs and priorities. The *current* profile captures the organization's existing cybersecurity posture, while the *target* profile describes desired states that address gaps or new objectives. If a gap exists between the current and target profiles, organizations can find a way to bridge it by focusing on the most critical areas first.

Organizations can use the CSF to prioritize issues for mitigation. For example, they might do the following:

- Implement encryption protocols to secure data transmissions.
- Deploy intrusion detection systems at ground stations.
- Design fail-safe mechanisms that prevent unauthorized commands from affecting satellite operations.

Ongoing monitoring and periodic reassessment keep the risk assessment process dynamic and responsive to emerging threats.

Threat Modeling with OWASP Threat Dragon

Threat modeling is the process of systematically identifying and addressing potential security threats to a system throughout its life cycle. Unlike risk assessment, which evaluates the likelihood and impact of known risks, threat modeling is proactive; it aims to anticipate how a system might be attacked and to design protections early in development. The results of threat modeling can even serve as inputs to a risk assessment, helping prioritize risks and determine mitigation strategies.

A typical threat modeling process begins by defining the system in question, then identifying potential threats. Well-known frameworks such as STRIDE (which categorizes threats into categories such as spoofing and tampering) or PASTA (a more risk-oriented approach) can serve as guides. Next, the organization should plan mitigations and review the model iteratively to identify any remaining gaps.

It can be helpful to visualize this process using tools like OWASP Threat Dragon, which allows users to create diagrams of a system's components and trust boundaries. As an example, we'll walk through a threat model of a space system using Threat Dragon and the Space Attack Research and Tactic Analysis (SPARTA) framework. SPARTA is a space-specific threat identification and response framework which we will discuss in more detail in "Standards and Frameworks" on page 292.

To get started with Threat Dragon, navigate to *https://owasp.org/www-project-threat-dragon/* and choose your preferred deployment method. You can install it locally or run it in a Docker container. Next, either start the web server or run the installed application to access a menu where you can open an existing threat model, create a new one, or explore a sample.

We encourage you to check out the included sample threat models to get a sense of the tool's capabilities before you create your own model. The demo threat model in Figure 2-2 shows a web application with background workers and a message queue.

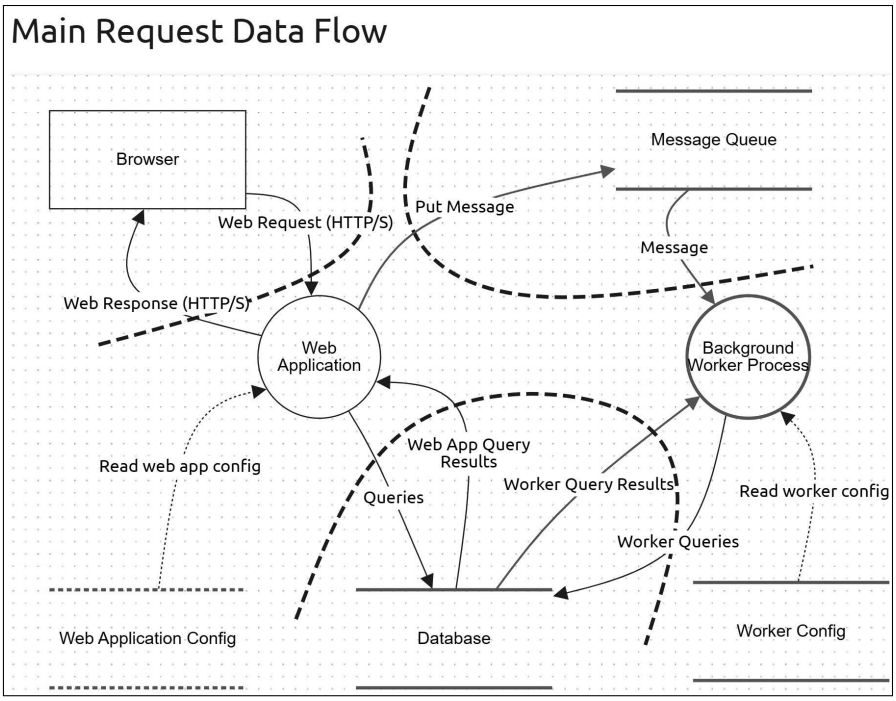

Figure 2-2: A demo threat diagram

On the left side of the screen, you'll see the components you can include in a diagram. A *process* typically represents something internal to the system and within its control. A *store* represents a database, such as those used in a ground station to store telemetry. *Actors* indicate someone or something interacting with the system or software. In our case, this could be a spacecraft controller. Data flow is represented using arrows between components, which default to unidirectional but can be changed to bidirectional.

You can draw trust or privilege boundaries as either boxes or lines. These boundaries delineate areas where privileges begin or end and where entry or exit points for your application or system exist. Finally, the descriptive text box lets you add additional annotations or explanations. If, for example, you want to keep a diagram focused on a specific type of threat or data flow, you might leave some components out of scope and use a text box to explain your reasoning.

Now that you know the components you can use in a diagram, create a new threat model using the dialog shown in Figure 2-3.

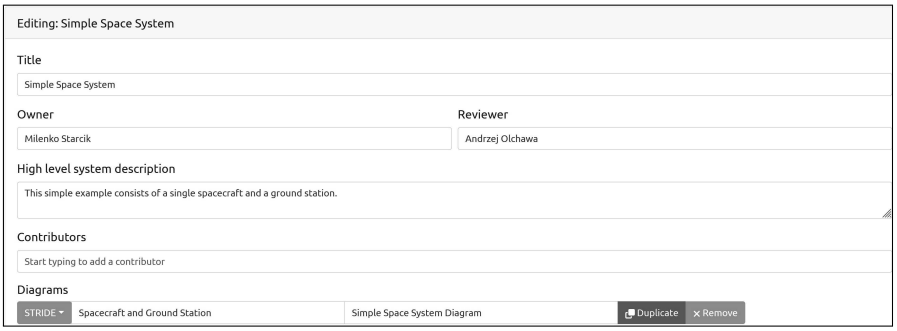

Figure 2-3: Creating a new threat model

Provide a title for your new model and fill in the names of the owner and eventual reviewer. Next, write a concise, high-level description of the system you want to model. Choose the type of diagram to create (in this case, STRIDE), and give the diagram a name and a brief description. You can add multiple diagrams to one threat model. Save the information, then click **Close** to return to your thread modeling project overview.

Click the STRIDE diagram to open it for editing. You should see an empty diagram, as in Figure 2-4.

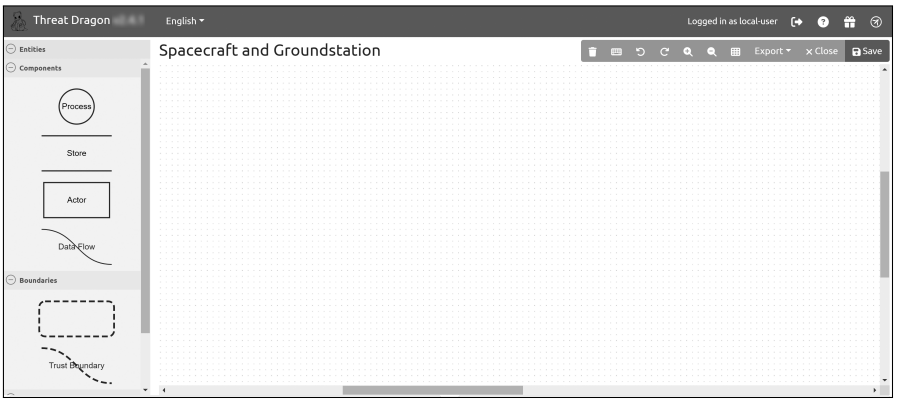

Figure 2-4: An empty STRIDE diagram

Now it's time to model your space system. In Figure 2-5, we've created a simple example to get you started. Begin by placing the processes and actors, then connect them with data flows and add the trust boundaries.

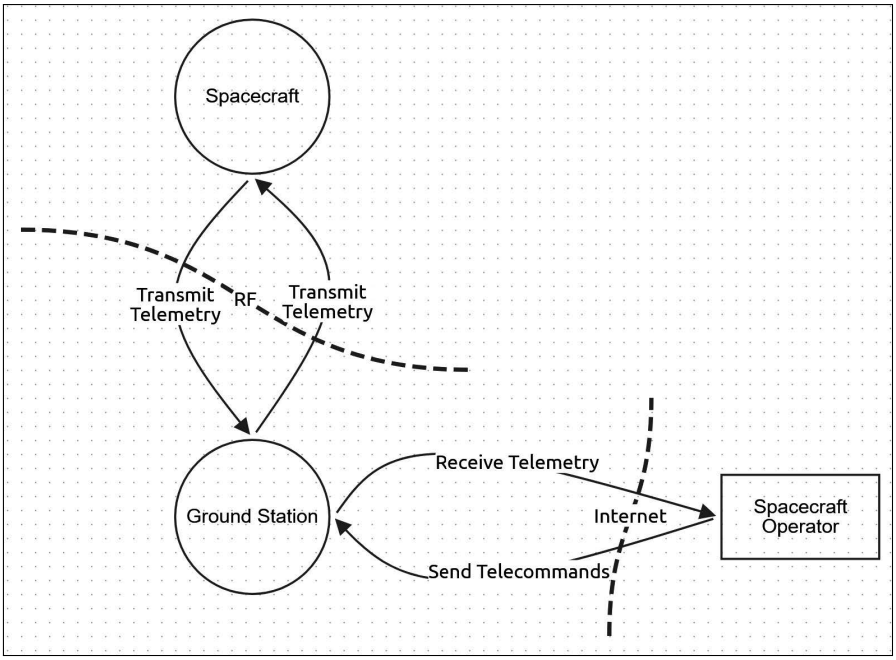

Figure 2-5: Beginning a diagram

Once you've created a diagram, you can choose a component and add a new threat to it. We've chosen to add compromise of our ground station infrastructure (Figure 2-6). If you leave the status as "not mitigated," Threat Dragon will highlight it in red until you mitigate it.

From the overview menu, you can create a report using the button at the bottom right. The report provides a summary of the identified threats, images of the diagrams, and a table listing the threats associated with each element.

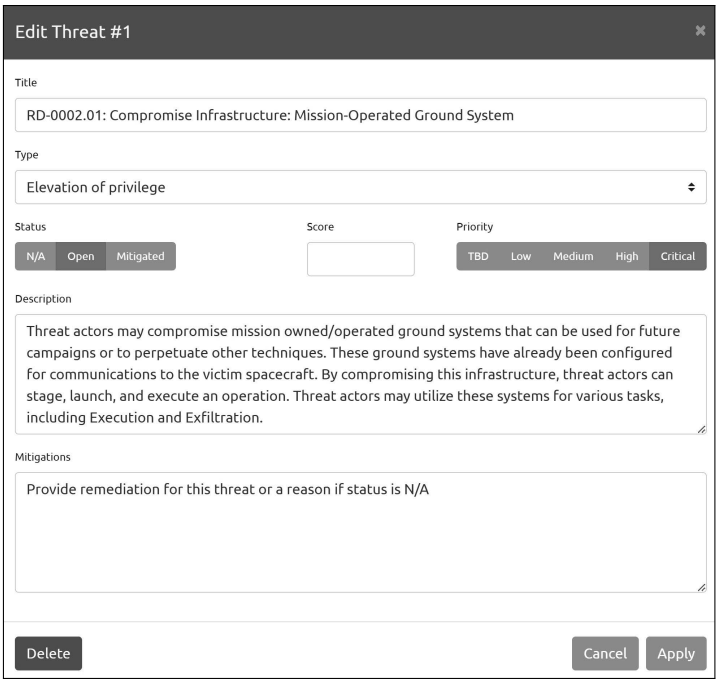

Figure 2-6: Adding a new threat

This covers the basics of creating a space system threat model in OWASP Threat Dragon. In threat modeling, there is no single correct approach. Different methods can be applied, and you can adapt tools like Threat Dragon to fit your specific application.

Conclusion

The ever-evolving space threat landscape challenges organizations, governments, and individuals across the industry. As this chapter has shown, the increasing sophistication, frequency, and diversity of threats, from physical attacks to ransomware to nation-state attacks, underscore the urgency for proactive, adaptive, and intelligence-driven defense strategies. Understanding the motivations of threat actors, anticipating emerging threat vectors, and fostering a culture of security awareness are no longer optional. Going forward, sustained collaboration across sectors, continuous monitoring, and investment in resilient and innovative security technologies will be essential to maintaining the safety and sustainability of space operations.