CSS Analyses in Security Policy

No. 343, June 2024

Understanding Cybersecurity in Outer Space

Cyberspace and outer space share many similarities due to their open, shared, expansive, transboundary, and intangible nature. The digitalization of space has increasingly interlinked space and cyberspace, exposing satellites, ground stations, and user terminals to cyber threats. Understanding the links between space and cyberspace is critical to better protect the space assets on which society relies.

By Clémence Poirier

On 24 February 2022, hours before the invasion of Ukraine, a cyberattack targeted Viasat's KA-SAT satellite network, which was used by the Armed Forces of Ukraine. The attack was designed to prevent Ukraine from using space to respond to the invasion, but it also created ripple effects throughout Europe, affecting thousands of civilian customers across the continent, including critical infrastructures. This attack shed light on the vulnerability of space systems to cyber threats.

Satellites, like any digital object, can be hacked. However, because they are so removed from most people's daily experience, it can be easy to overlook just how much societies rely on them. If GPS were to be unavailable, the economic impact in the US alone could reach 1 billion USD per day. A cyberattack on a satellite may significantly disrupt financial markets, road transportation, weather forecasts, internet connection, electricity grids, air control, and military operations simultaneously.

Two satellites in outer space juxtaposed on a background of lines of programming code. *Generated using DALL-E OpenAI*

While this threat is not new, the risks have increased due to the digitalization of space systems and the space sector at large. Satellites are now frequently equipped with software components and are connected to the internet. In addition, most processes in the design, manufacturing, testing, launch, and operations of satellites rely on digital technologies. For example, recently the first Bluetooth connection to a satellite over 600 km away was established. Satellites can therefore be regarded as expensive computers flying in orbit, which can be hacked like any other connected device. This has led to an extension of the attack surface, which refers to all the entry points that can be exploited by an attacker to disrupt, damage, disable, or take control of a satellite.

The inherently adverse nature of outer space (e.g., long distance from Earth, cosmic rays, extreme temperatures, radiation) creates a set of unique policy, legal, technical, and commercial challenges in a sector that has long overlooked cyber threats. In addition, the cybersecurity of space systems is not limited to the satellite in orbit but comprises the supply chain, the user, ground, and space segments throughout their entire lifecycles, creating additional layers of complexity.

This analysis will look at the evolution of the telecommunications sector, the evolution of the threat landscape in space, the specific cyber threats affecting space systems, and the policy, regulatory, and commercial issues that come with them. Finally, this paper will provide an outlook on how Switzerland may seek to address these vulnerabilities.

Militarization vs. Weaponization of Space

The militarization of space describes the use of space for military operations on Earth. In the 1950s, the militarization of space began, coinciding with advancements in ballistic missiles and nuclear weapons. In the 1990s, discussions regarding the militarization of space shifted to primarily focus on operational aspects. Satellites emerged as essential enablers of military operations on Earth. From 2022, discussions regarding militarization have focused on commercialization, with belligerents relying on commercial services rather than military-owned systems.

The weaponization of space implies the placement and/or use of weapons in space. This is an emerging phenomenon, which is latent but not yet happening. The deployment of weapons in space is not forbidden by international law; only the deployment of weapons of mass destruction is as per the Outer Space Treaty of 1967.

A Merging of Cyber and Space

The telecommunications sector has evolved significantly in the past two decades and space systems are now an integral part of the broader digital infrastructure. While submarine cables and terrestrial fibers account for most internet traffic, satellites' shares of web activities have gradually increased in the past five years. This is due to the shift of the telecommunication satellite market. It used to rely on a few geostationary satellites to provide broadcast services, including direct-to-home and direct broadcasting services. With the advent of large commercial constellations in Low Earth Orbit, the market transitioned to providing internet broadband services, including direct-to-device services.

Satellites have also been increasingly integrated into terrestrial telecommunications, including 5G and 6G mobile networks. The role of satellites will likely continue to increase in internet infrastructure, including beyond Earth. For instance, NASA and ESA are developing standards for LunaNet to provide network connectivity on the Moon.

Threat Landscape

The threat landscape in space has evolved. Space has become congested; Earth's orbit now contains approximately 9,000 operational satellites, 100 million pieces of debris of approximately 1 millimeter in diameter, 500,000 pieces of debris sized between 1 and 10 centimeters, and 30,000 pieces of debris over 10 centimeters. Space has also become competed, with an increasing number of both public and commercial space actors. Space is likewise contested. States have monitored an increase in anti-satellite tests (e.g., China in 2007, India in 2019, Russia in 2021) hostile maneuvers and inspection missions with attempts to eavesdrop on other space assets (e.g. Luch-Olymp), the release of projectiles (e.g., Kosmos-2523), and the deployment of highly maneuverable space planes along with new active defensive and offensive postures in military doctrines.

Most incidents do not target the satellite in orbit but rather the ground station or user terminals.

The cyber threat landscape in space has also evolved. At the dawn of the space age, it focused on electronic threats between Soviet and US systems. From the 1980s, it largely centered on electronic threats and the interception of satellite data by pirates and amateur hackers as well as interference with satellite broadcast in the context of the Cold War (e.g., illegal broadcast of propaganda). From the 1990s, the rise of satellite broadcast led to a spike in satellite TV piracy. The 2000s saw a rise in "spoofing" from non-state actors as well as state-sponsored attacks mostly targeting the ground segment. From the 2010s, cyberattacks have continued to increase in volume and complexity, targeting both commercial and state-owned systems across the entire attack surface and coming from an heterogeneous pool of threat actors.

Today, the threat landscape is characterized by a better understanding of the dependence to space in society and the military, making satellites tempting targets for threat actors. This is coupled with a rise in hacktivism, with many groups taking sides in armed conflicts (e.g., Killnet targeting Starlink as part of the war in Ukraine). Criminal groups are now regularly targeting space companies (e.g., Lockbit targeting SpaceX and Boeing). Thus far, attacks have usually generated temporary and reversible effects. Most incidents do not target the satellite in orbit but rather the ground station or user terminals.

The number of cyberattacks targeting space systems has recently skyrocketed. However, it is difficult to provide detailed numbers. This is due to the fact that most space companies used to be defense companies, which relied on the assumption of achieving security by obscurity. They avoided sharing information, reporting attacks, or disclosing data about their companies or systems to prevent any malicious exploitation. Additionally, no legal obligations compelled them to report attacks to authorities or customers.

Some scholars and companies attempted to map cyberattacks against space systems, and the results illustrate the changing threat landscape well. Pavur and Martinovic's database counts 113 attacks from 1957 to 2022. Market intelligence company CyberInFlight reports 337 cyberattacks since the 1970s, 90 of which took place in 2023, and 30 in the month of January 2024 alone. Disparities in numbers pertain to the lack of public information and various methodologies. Furthermore, these are likely low estimates as attacks remain underreported. At the national level, methods and data vary even more. NASA declared 1,785 cyber incidents in 2020 alone (including equipment loss and theft).

What is so Special about Space?

Cyberattacks on space systems can affect strategic stability in outer space, unlike kinetic threats. Strategic stability in space has been maintained over the years thanks to limited accessibility to space and space technologies, and limited access to anti-satellite (ASAT) capabilities. In addition, kinetic ASAT can be monitored and attributed by any country with radar capabilities, rendering plausible deniability impossible. Furthermore, a kinetic ASAT hit usually creates space debris which will indiscriminately affect other satellites in orbit. Cyber threats constitute a paradigm shift because cyber offensive tools are easily accessible to all; cyberattacks are difficult to attribute and plausible deniability is always possible; and cyberattacks on space systems do not generate debris and therefore do not affect the attacker, which can incentivize irresponsible behavior in both space and cyberspace. Moreover, many critical infrastructures rely on satellite connectivity to function. A single cyberattack on a satellite may impact the functioning of several critical sectors at the same time.

Policy Issues

Until 2019, public policies worldwide largely neglected to consider cyber threats to space systems. Scholars brought attention to this blind spot, suggesting that cyber risks on space systems were too simplified, misunderstood, and that cyber and space policies were incompatible with one another. Since then, states have progressively recognized the threat in their public policies.

Consequently, major spacefaring nations started to adopt space defense strategies, in addition to their regular space policies, to respond to the changing threat landscape. In 2019, France released its Space Defence Strategy, which acknowledged cyber threats on space systems and recognized them as one of the most likely threats. In 2019, Italy adopted its National Security Strategy for Space to respond to unintentional and intentional threats, including cyber ones. In 2022, the UK adopted its Defence Space Strategy, which underlined the damaging potential of cyber threats on the UK's ability to conduct military operations. It also highlighted the development of cyber capabilities by potential adversaries that may target UK space assets. However, most policy documents outlined few specific measures to counter cyber threats beyond adopting a counter offensive posture (e.g., France, Italy), integrating space in cyber exercises (e.g., UK), hardening (e.g., France), or retaining capabilities to operate in degraded environments (e.g., France).

A single cyberattack on a satellite may impact the functioning of several critical sectors at the same time.

In 2020, the US adopted Space Policy Directive 5, which is a dedicated policy providing overarching cybersecurity principles for space systems. The Space Force's Spacepower Doctrine doctrine highlights cyber operations in space as an essential aspect of military space operations to retain space dominance, which is then delineated in the Space Force's doctrinal documents for both defensive and offensive actions.

Emerging spacefaring nations, which have more capabilities in the cyber domain than in the space domain such as Estonia or Israel, have decided to make cybersecurity a pillar of their space policies and use it as a springboard to develop their space programs.

The cyberattack on the Viasat satellite prior to the invasion of Ukraine constituted a wakeup call for EU policymakers. The EU's Strategic Compass, Policy on Cyber Defence, and Space Strategy for Security and Defence all reference cyber threats on space systems as significant, pernicious, and likely. The latter recommends implementing security-by-design, systematic integration of cybersecurity standards, exchange of best practices among commercial entities, consistent security monitoring of all EU space programs, and the integration of cybersecurity measures in a new space legislation.

Regulatory Issues

In Europe, regulatory frameworks for space cybersecurity remain limited. While 11 European states adopted a space law, none of them integrate legally binding cybersecurity measures.

At the EU level, in 2022, the NIS2 Directive recognized space as a sector of high criticality and required "operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services" to implement stricter cybersecurity measures and reporting mechanisms. However, as a directive, it must be implemented through national laws, and almost no EU state has done so to this day. Additionally, there is still room for interpretations regarding the scope of its implementation. For instance, whether "ground-based infrastructure" also encompasses the user and space segments. NIS2's measures are also very general and are not necessarily adapted to the specificities of space systems. The sector will likely need support for implementation.

The EU is also in the process of developing space legislation that is expected to integrate cybersecurity measures. In parallel, several EU Member States are beginning to update their own national space laws to include cybersecurity measures but await the EU legislation first. While the EU initially planned to introduce the bill in March 2024, it later postponed it to at least summer 2024.

It is important to note that developing dedicated cybersecurity standards for space systems has been a rather slow and cumbersome undertaking. Traditional cybersecurity standards are often inadequate and do not consider the specific nature of space systems and the orbital environment. Some entities (e.g., Consultative Committee for Space Data Systems) have only recently developed standards specific to space systems, which have yet to be adopted across the industry.

Technical Issues

Cybersecurity on Earth is different from cybersecurity in space. From the moment the spacecraft is launched, it cannot be accessed and components cannot be removed and replaced in case of vulnerability or malfunction. While on-orbit servicing holds promise for conducting such operations, the market is not yet mature. The satellite cannot be unplugged like a computer on Earth.

In addition, computing power on board the spacecraft is limited, which means that the use of long cryptographic keys can become a constraint as it may deplete the satellite's limited power source.

The digitization of space systems heightens their susceptibility to conventional cyber threats, necessitating the implementation of traditional cybersecurity protocols. However, the distinct characteristics of space systems also reveal the inadequacy of traditional cybersecurity measures. For example, end-to-end VPN encryption, which is very common on computers on Earth, is not suitable for satellites due to their far distance from Earth, resulting in the loss of data packets.

Commercial Issues

In the industry, cybersecurity was long overlooked as operators (and customers) preferred latency and efficiency over security. Today, major space companies seem to have developed a good awareness of cyber threats. The difficulty is rather for start-ups, which often prefer to focus on mission specifics or do not have the resources to integrate cybersecurity.

To face cyber threats, industry-led initiatives have been established, such as the Space Information Sharing and Analysis Center (ISACs) to share cyber threat intelligence, vulnerabilities, and information between members and government authorities. The EU, for example, decided to establish a Space ISAC in 2023. However, its governance is still undecided, including the potential integration of non-EU European entities such as Switzerland, Norway, or the UK.

The demand for space cybersecurity is rising, creating an emerging market comprising new, dedicated space cybersecurity companies; traditional IT companies attempting to enter the space market; and major space companies working to commercialize space cybersecurity services. This industry is expected to generate 33.2 billion USD in the next ten years, providing opportunities for innovative countries such as Switzerland.

What is at Stake for Switzerland?

Similar to many other European states, Switzerland does not have sovereign satellites. Nevertheless, Switzerland is pursuing activities in space, as illustrated by the launch of three Belgian satellites carrying a Signal Intelligence payload from the Swiss Armed Forces in March 2024. As a result, Switzerland is still vulnerable to cyber threats as there are about 160 Swiss companies involved in the space supply chain. Various critical sectors in the economy rely on foreign satellite services to function (e.g., banking, transport, logistics, and the armed forces). The functioning of these important industries, then, ultimately relies upon cybersecurity measures implemented by foreign actors.

Developing dedicated cybersecurity standards for space systems has been a rather slow and cumbersome undertaking.

This is a domain that caught the attention of policymakers in 2021, prompting the Federal Council to issue a report on cyber risks in space at the request of the Swiss parliament. In May 2024, the National Council's Security Policy Committee, based upon the conclusions of the report of 2021, submitted a motion suggesting that the Federal Council further cooperate with the EU in the field of space in light of its growing role in security policy. However, the motion addresses space more broadly and is not focused on space cybersecurity.

At the policy level, the Swiss Space Policy of 2023 briefly addressed the possibility of cyberattacks on satellites. However, it does not include any measures to ensure the cybersecurity of the Swiss space sector. Other public policies also do not address space cybersecurity. At the legal level, Switzerland does not yet have a space law, but is in the process of drafting one. It remains to be seen whether cybersecurity will be included.

Outlook

As the threat landscape in space evolves, so should the understanding of cyber risks and their mitigation measures to protect space assets and the broad range of services they provide to society. Upcoming challenges in space cybersecurity will pertain to bridging the skill and information gap, developing an adapted legal framework, and ascertaining how to most effectively conduct and respond to cyber operations in space.

For more on perspectives on cyber security, see CSS core theme page.

Clémence Poirier is a Senior Researcher in the Cyberdefence Project with the Risk and Resilience Team at the Center for Security Studies (CSS) at ETH Zurich.

CSS Analyses in Security Policy is published by the Center for Security Studies (CSS) at ETH Zürich. The CSS is a center of competence for Swiss and international security policy. Each month, two analyses are published in German, French, and English.

Editor: Névine Schepers
Language Editing: Ally Chandler
Layout and graphics: Miriam Dahinden-Ganzoni

Feedback and comments: analysen@sipo.gess.ethz.ch
More editions and online subscription: www.css.ethz.ch/cssanalyses

Most recent editions:

Pyongyang's Relations with Moscow and Beijing No. 342
Comparing Critical Infrastructure Policy Updates No. 341
European Security Cooperation with the Indo-Pacific No. 340
Heightened Nuclear Risks and the Risk Reduction Agenda No. 339
Knowledge Security at Stake No. 338
Strategic De-risking Beyond Chips No. 337

ISSN: 2296-0244; DOI: 10.3929/ethz-b-000675292