N°4 - JANUARY/MARCH 2025

CYBER-IT

CYBER IS A MARATHON NOT A SPRINT !

DESTINATION MOON
Are we ready to live on the moon ?

INSIGHT
Who better than an astronaut to take us beyond the stars ?

DATA CENTERS
Our data in space

STARLINK
A prime target ?

SPECIAL REPORT

CYBERSECURITY IN SPACE

Inquiry / Requests?
cyberit.magazine@gmail.com

EDITO

You might be wondering : “why focus on cybersecurity in space?”

Quite simply, after a discussion with friends and a quick look through my LinkedIn contacts, the idea came to me naturally. However, having an idea is great, but putting it into action is a whole different challenge! I had to put in a lot of effort to find concrete information and connect with people who could, and most importantly, were willing to give me an insight into their profession.

It was not easy...the space industry is complex and often impenetrable. Information needs to be secured at all times for obvious safety reasons. Of course, I will not dive into the very technical or secret details about satellite manufacturing, but I tried to get into this fascinating universe that many of us find so extraordinary.

I have several contacts who work in this field, so I relied on their expertise and knowledge to remain as close to reality as possible while addressing the various topics featured in this issue. Additionally, with a bit of perseverance and persuasion, I got to interview one of the pioneers of French space exploration, a man who made his wonderful dream come true : traveling into space!

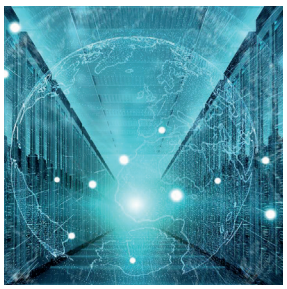
Thank you to all the contributors to this new issue, I hope you enjoy reading it as much as I enjoyed writing it.

ARNAUD LEROY

Solidarity Sponsorship Campaign !

Would you like to see your logo featured in the magazine or highlight a project through a publication ? Let’s make it happen ! Simply contribute by donating to one of the charities selected by the Cyber-IT Ethics Committee, and that’s it. It’s a win-win project: a meaningful gesture to help those in need. (For more information, visit the Cyber-IT LinkedIn page or contact us by email.)

SOMMAIRE



IN SPACE

With THALES ALENIA SPACE - CNES - CYSEC - ETH ZURICH

CYBERSECURITY IN SPACE

Many thanks to the various experts and the CYSEC for their assistance and availability to work on this special report :

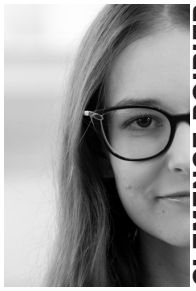
STEPHANE DESCOUS

THALES

ThalesAlenia Space

JULIEN AIRAUD

cnes CENTRE NATIONAL D'ÉTUDES SPATIALES



CLEMENCE POIRIER

ETH zürich

Stéphane Descous is the Director of Product Cybersecurity at the Thales Group since January 1, 2025, based in Toulouse, France.

Prior to this, he spent nearly seven years at Thales Alenia Space (TAS), where he held various key positions in cybersecurity.

He served as the Cyber Internal Auditor for the GALILEO program, Head of Cybersecurity for the Navigation France division, and then Chief Product Security Officer at TAS, playing a cross-functional role within the company.

He holds a Master's degree in Economic and Legal Expertise in Information Systems.

Julien Airaud is a Senior Space Cybersecurity Expert at CNES (French Space Agency).

For nearly fifteen years, he has led projects in the cybersecurity of orbital systems and launch systems. He is now in charge of future preparedness activities in this field.

Holding a Master's degree in Information Security from the University of Limoges, France, he is involved in projects with various higher education institutions.

He regularly moderates, contributes to, or participates in various forums or events focused of space and cybersecurity.

Clémence Poirier is a Senior Researcher in Cyber Defense at the Center for Security Studies (CSS) at ETH Zurich.

Her research focuses on space cybersecurity, electronic and cyber conflicts in space, as well as broader issues of space security and defense.

She holds a Master's degree in International Relations, International Security, anDefense, as well as a Bachelor's degree in Applied Foreign Languages (English, Russian, Spanish) from the University of Jean Moulin Lyon III, France.

SPECIAL REPORT

Celestial Strategic Stakes

Since the early stages of space exploration, space has become an unprecedented area of exploration and competition.

The satellites navigating the skies now have evolved rapidly. They play a crucial role in our daily lives, providing essential services such as communications, satellite navigation (GPS), weather forecasting, Earth observation, and much more.

The omnipresence of satellites in our society has made them a prime target for malicious hackers. Space, once considered a sanctuary, has become a new battleground, where economic, political, and strategic stakes are high.

The massive investment from nations and companies in developing space capabilities, combined with the current geopolitical landscape, has increased competition and intensified the risk of conflicts.

At the same time, satellites have become more advanced and digital. Smaller electronic components, sophisticated software, and operating systems have significantly boosted their performance.

However, this digital evolution has also made satellites more vulnerable to cyberattacks.

In many ways, satellites are now like flying computers, facing similar threats as ground-based systems, such as viruses, malware, and hacking.

The growing connection between satellites and ground infrastructure has also created new weak points.

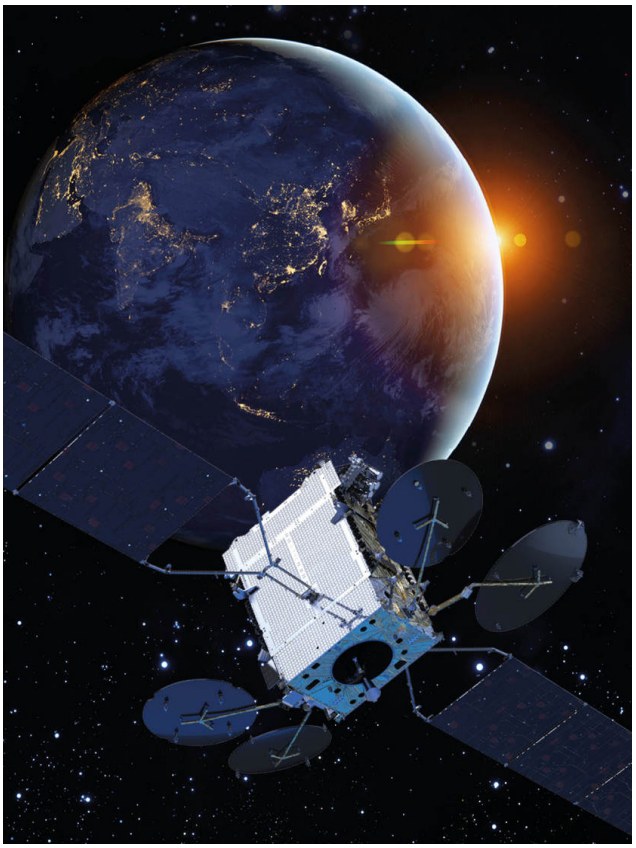
Data collected by satellites is sent to ground stations and then shared through terrestrial networks or other satellites.

This interconnected system gives attackers more chances to breach space systems and disrupt their operations.

As **Stéphane Descous**, former security chief at Thales Alenia Space, explains, the key challenge is improving how we detect threats in space.

Losing our connection to space systems today would be disastrous because so much of our modern world depends on them.

We must also remain vigilant about the various manipulations of the information we receive. It is crucial to make independent and informed decisions in situations where we need to take action.



In the 1990s, the European Union found itself heavily dependent on the United States for satellite navigation technologies.

While the performance of GPS was considered sufficient for everyday use, improvements were necessary to support more demanding applications in civil engineering, agriculture, and transportation, and

to meet high-security requirements. This need led to the launch of the EGNOS (European Geostationary Navigation Overlay Service) project.

By 1999, a report from the French National Assembly on the Kosovo War highlighted growing concerns about the increasing reliance of military equipment, such as missiles and aircraft, on GPS, which was "entirely under American control."

In response, the European Union initiated the Galileo project in 2001. Galileo provides highly precise location capabilities, offering an alternative to GPS and strengthening Europe's independence in satellite navigation technologies.

Several other programs and ambitious projects to develop Europe's own space capabilities are currently underway.

These initiatives aim to provide secure connectivity services to the EU and its member states, as well as connectivity for government authorities, private companies, and citizens.

Clémence Poirier sheds light on this issue, using the attack on the KA-SAT network as an example: "A few hours before the invasion of Ukraine, Russia launched a cyberattack on the KA-SAT satellite network operated by the American company Viasat.

The attack began as a denial of service targeting user modems, followed by the exploitation of a vulnerability in the VPN network of the ground segment operator for KA-SAT. This allowed the deployment of a 'wiper malware,' which erased the hard drives of all user modems, including those used by the Ukrainian military.

Following this incident, I identified 124 cyber operations targeting the space sector in connection with the war in Ukraine.

There are likely many more, as numerous operations are not made public.

In total, 57 different entities were targeted, including Starlink, NASA, Lockheed Martin, Boeing, the European Space Agency (ESA), the Swedish Space Agency, and others. 61% of these operations targeted private space companies, 32% targeted space agencies, and 3% targeted research institutes.

This is not surprising given the widespread use of commercial space services in the conflict."

The primary risks identified in the space sector have evolved over time. Over the past forty years, attacks mainly focused on the ground segment, often involving espionage by both state and non-state actors. Jamming operations were also observed, though they typically remain out of sight unless they involve lasers, which can occasionally target satellite optics.

Today, satellites can be destroyed from Earth, but this comes with significant consequences. Such actions produce debris that can collide with other countries' satellites, causing severe repercussions. However, the impact of these attacks cannot be precisely controlled or predicted. Additionally, a satellite can be rendered inoperable without being destroyed, making it just as uncontrollable and dangerous.

Satellite hijacking can be divided into two categories:

Systems control: This involves taking control of the hardware to deviate it from its original purpose. For instance, an attacker could alter a satellite's trajectory or push it out of orbit.

Payload control: This targets the satellite's primary functions, such as observation capabilities. Manipulating observation to avoid monitoring a specific area at a particular time can be highly advantageous for certain organizations or states.

SPECIAL REPORT

In the context of the Russia-Ukraine conflict, distributed denial-of-service (DDoS) attacks account for 65% of cyber incidents, while 11% involve intrusions and 9% are data breaches. Wiper malware, though impactful, remains a rare form of attack, with no additional cases identified to date.

Most cyber operations against the space sector have been relatively straightforward, causing only temporary disruptions.

The identified operations are almost all conducted independently of battlefield operations. Based on public data, no cyberattacks on space systems have been carried out as part of coordinated joint operations

However, many operations are connected to events in the conflict. For instance, the Finnish satellite imaging company ICEYE was targeted after announcing its provision of satellite images to Ukraine.

Similarly, defense companies are frequent targets due to their production of equipment used in Ukraine, but attackers are sometimes surprised to find information related to space systems. This occurred during the pro-Russian Killnet group's attack on Lockheed Martin which is one of the key contractors behind many systems of NASA and the U.S. Air Force.

Information for the general public is not always easy to access on topics as technical and specific as space and satellite systems. However, organizations like CYSEC have been able to highlight events such as CYSAT, which bring together key players in the field and showcase the capabilities and advancements in this area.

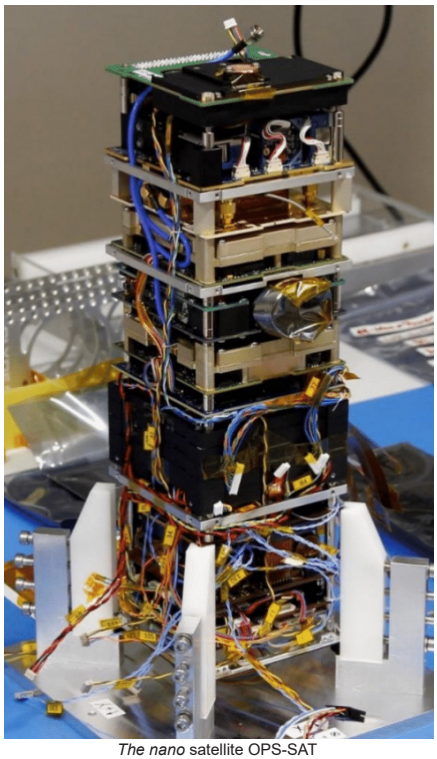
Mathieu Bailly, co-founder and director of CYSEC, explains that during the third edition of CYSAT, a European event dedicated to cybersecurity in the space industry, the European Space Agency (ESA) hosted a simulated remote takeover of the OPS-SAT satellite. OPS-SAT, a nanosatellite designed for demonstration purposes, became the subject of an offensive cybersecurity challenge.

Thales' offensive security team identified vulnerabilities that could disrupt the satellite's operations, showcasing how targeted exploitation could impact its functionality.

Participants employed various ethical hacking techniques to gain control over systems such as sensor management, geolocation, attitude control, and camera systems. These actions demonstrated how cyberattacks could lead to severe damage or even complete loss of satellite control.

This unique exercise mobilized Thales' offensive security team, with support from ITSEF (Information Technology Security Evaluation Facility), highlights the critical need for advanced cyber resilience tailored to the highly specific environment of satellites.

The Thales team, composed of four cybersecurity researchers, successfully breached the satellite's onboard system.



The nano satellite OPS-SAT

"

Ensuring consistent security is an essential part of our mission

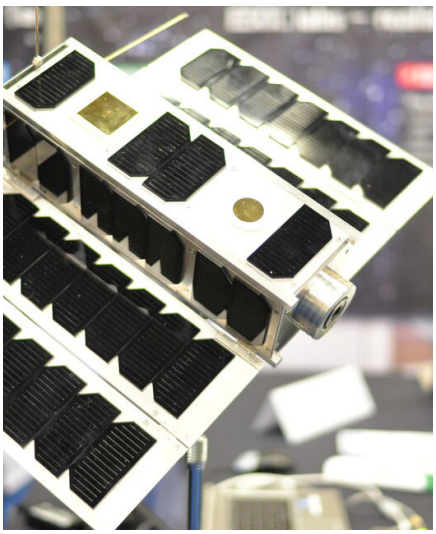
"

Julien Airaud
Space Cybersecurity Senior Expert - CNES

By leveraging standard access rights, they gained entry into the application environment and introduced malicious code by exploiting several vulnerabilities.

This allowed them to compromise the data transmitted back to Earth, including altering the images captured by the satellite.

They also achieved other objectives and could mask certain geographical areas in satellite imagery, all while concealing their activities from the ESA.



A model of satellite OPS-SAT

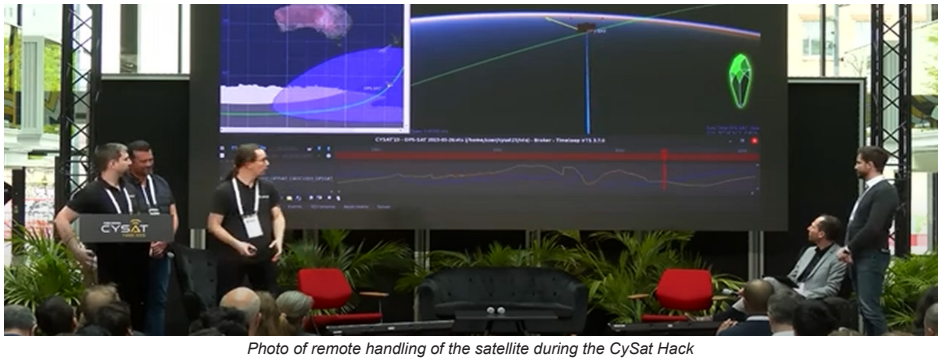


Photo of remote handling of the satellite during the CySat Hack

Main pillars to improve the safety of space infrastructure

Awareness and Threat Modeling

Being aware of cyber risks and regularly modeling the threats faced by the organization or agency. This threat model should be updated as frequently as necessary to stay relevant. en situation pour sans cesse améliorer ce plan et s'assurer d'un rétablissement rapide des systèmes.

Integrating Cybersecurity from the Start

Incorporating cybersecurity measures right from the beginning of the mission's design phase. This includes embedding security into the mission's architecture, often referred to as "cyber by design."

Maintaining Security

Ensuring continuous security maintenance. Once operational, systems need regular updates, patches, and maintenance to address emerging vulnerabilities and threats.

Preparation and Incident Response Planning

Preparing for potential attacks by having a robust incident response plan. This plan should outline roles and responsibilities during an attack, points of contact in governmental agencies, reporting obligations, and potential responses for various scenarios. Regular simulations and exercises are crucial to continually refine the plan and ensure the swift systems recovery after an incident.

SPECIAL REPORT

Could space be the new Wild West ?

Attacks on entire constellations are possible and can occur at various stages of a satellite's lifecycle. A satellite can even be targeted before its launch. The threat is significant, especially as time goes by and launch systems, satellites, and associated software become increasingly digitized.

Launch operations are protected by the French Armed Forces in French Guiana under the TITAN system, although the actual execution remains a civilian endeavor. In any case, the sector is secured by legionnaires, with the French navy also deployed in nearby waters. This was the case during the Ariane 6 launch.

170 legionnaires and surface-to-air artillery soldiers from the 3rd Foreign Infantry Regiment were tasked with preventing any intrusions into the protected zone. In the air, security was ensured by a Puma helicopter and two Fennec helicopters.

At sea, 30 sailors aboard the Antilles-Guyane Patrol Vessel (PAG) "La Confiance" and part of the crews from the coastal surveillance boats "Charente" and "Organabo" conducted patrols in the restricted maritime zone surrounding the space center.

At the slightest alert or suspicion, the teams react immediately, and in some cases, the entire process is shut down. Satellite constellations are designed to be resilient, meaning multiple satellites support the same service. If one satellite fails, another takes over, and so on. However, to ensure even a minimum level of service, several satellites are required.

A service cannot rely on just a single satellite. Systems (whether orbital or launch vehicles) are vulnerable during transportation, manufacturing, testing, final assembly, integration, and other stages. As a result, they require constant protection throughout their entire lifecycle.

An attack before launch is costly and time-consuming. Would the outcome be rewarding enough to justify such a logistics effort?

"

Clémence Poirier shares an example: in 2021, two laptops belonging to Ariane Espace employees, which were unprotected and contained confidential data about the Ariane 6 launcher, were stolen by a petty thief and later found in the basement of a housing complex of Paris suburban area, in Seine-Saint-Denis.

Fortunately, the thief likely had no idea about the assets he had in his possession, and the police were able to recover the laptops. However, had they fallen into the wrong hands, the stolen data could have provided critical information for a cyberattack.

This type of risk is far from uncommon. Between 2017 and 2020, NASA recorded between 274 and 430 instances of lost or stolen IT equipment, annually. These figures are classified by NASA as cyberattacks.

Given that satellites within a constellation are all identical, discovering and exploiting a vulnerability in one satellite

means it could potentially be exploited across the entire constellation. To date, there are no known cases of an entire constellation being taken over. However, such an operation would be highly complex to execute without detection.

When the war started in Ukraine, SpaceX reported having to allocate additional resources to support its cyber defenses and anti-jamming measures in response to an increased level of threat. It is important to note, however, that in the course of my research, I have not found any instances where the entry point for an attack was the space segment (the satellite in orbit). All the identified attacks targeted either the equipment used by end-users, the systems on the ground that control satellites, or the IT infrastructure of the companies managing them. Simply targeting the systems and networks on the ground is enough to disrupt how satellite networks function.

"

Julien Airaud, Senior Expert in space cybersecurity at CNES (Centre Nationale d'Études Spatiales), provides further details on security:

"Our field of activity, space, is not accessible to everyone: the environment is highly restrictive, and the technologies we can deploy, especially in cybersecurity, are limited by the size/weight/power ratio of the vehicle.

Access to space is becoming more accessible, and the number of objects in orbit (both useful and debris) is growing exponentially. Since international law assigns responsibility for potential damage to the operating country and space must remain a usable domain, states require space operations to be licensed. Obtaining these licenses may sometimes depend on the operator's compliance with cybersecurity requirements.

Among these requirements are the implementation of basic IT protection measures, which are much more complex to apply to a spacecraft. For this reason, many protocols have been developed and standardized for the space domain, after extensive testing between agencies to address the interoperability constraints of missions and the environment (available power, propagation delays, etc.).

Several international groups are working on standardizing technologies for space: CCSDS (the Consultative Committee for Space Data Systems), ECSS (European Cooperation for Space Standardization), ISO (International Standards Organization), and IEEE (the Institute of Electrical and Electronics Engineers) have varying degrees of involvement in space cybersecurity.

Historically, the main focus has been to protect communication links between the ground and spacecraft, and also between vehicles, using methods to verify identities and encrypt communications.

We still rely on widely used encryption standards like AES (Advanced Encryption Standards). Master keys are often loaded on the ground, but once these keys are stored on a satellite, it becomes vulnerable if they are exposed.

This makes key management a critical concern for us. There's also a push toward adopting asymmetric cryptography, which is currently lacking in the space sector. The complexity arises because payloads and platforms need to communicate with each other, often involving thousands of connections.

To address this, we're now working on post-quantum cryptography and onboard intrusion detection systems. Our biggest challenge is the lack of protection measures.

This often stems from operators assuming that satellites are isolated and untouchable, neglecting the vulnerabilities of ground systems. To address this, CNES is getting prepared to release cybersecurity hygiene guidelines for space systems, in the near future."

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES

MICHEL TOGNINI

Beyond Earth: a French Pioneer's journey into space

We sat down with this pioneer and discussing his career and his vision for the future, particularly with the latest advancements in space exploration. Here's our conversation with the man behind the astronaut, someone who always looks ahead and is committed to sharing his knowledge and legacy.

" Believe in your dreams and don't give up too soon ! "

Hello Mr. Tognini, thank you for joining us in this special issue. Could you please introduce yourself ?

Hello.
I studied in the Paris region (France), specializing from third grade to high school to prepare for a career in engineering. I then spent two years in preparatory classes for mathematics at the “Pupilles de l'Air School” in Grenoble, France.

This military-focused school prepares students for the French Air Force Academy. I chose this path because I wanted to become an engineer and pursue a career in aeronautics. My love for aviation led me to join a military school where I could satisfy my passion for flying aircraft and practicing extreme sports.

After graduating from the Air Force Academy, I gained experience as a fighter pilot, initially flying the SMB2 and then later the Mirage F1. My expertise opened the doors to the test pilot school in England. With three years of experience as a chief test pilot, I seized the opportunity to apply for astronaut selection. I was selected in 1985 but had to adjust my plans following the Challenger shuttle disaster.

Then, I trained and flew in Russia before participating in a U.S. space mission in 1999.After the Columbia incident, I dedicated my career to training future European astronauts as the director of the European Astronaut Centre.

Can you briefly tell us about your missions in space ?

Indeed, I participated in two space missions: Soyuz TM-15 in 1992 and STS-93 in 1999.

The first was a French-Russian mission in July 1992, marking an important step in French space history. It led to significant progress in several areas, particularly through experiments on plant growth in microgravity, plant cells, and the effects of microgravity on various physical processes. As a scientist, I was deeply involved in this project.

My second flight took place exactly seven years after my first one, in July 1999. I served as an “ambassador” for France, as I was the first French astronaut to join the MIR space station. One key moment was my conversation with President Mitterrand, which history regards as a powerful symbol.

We had to launch the Chandra telescope to deploy it and place it into orbit. This mission was also a first in another significant way: Eileen Collins became the first woman to command a shuttle. It was a remarkable achievement !

Fifteen days in space, doesn’t it feel short after training for so many years ?

I would say it’s a progression over time. Back then, 15 days was the average duration for space missions. Today, missions typically last around six months, and in the future, they will be even longer.

In fact, studies are already underway to understand how the human body will adapt during extended crewed missions, such as the Mars 500 project. Mars 500 was an ambitious simulation of a manned mission to Mars, conducted on Earth between 2010 and 2011. Its goal was to test the psychological and physiological resilience of a crew confined to an environment mimicking the conditions of a long-duration space journey to Mars.

Looking back on my missions, I would say we were incredibly fortunate to be selected and to witness things very few people ever have the chance to see. Orbiting the Earth 16 times a day gave me the opportunity to observe regions I would never have been able to see with my own eyes otherwise.

So yes, it is many years of training, but it is absolutely worth every moment to experience something so extraordinary.

Michel Tognini

Your second mission to deploy the Chandra telescope faced numerous unexpected challenges. Did fear ever cross your mind during those moments ?

We lift off with confidence, surrounded by the support of engineers, friends, fellow astronauts, families, and many others. It is true that there were several unexpected delays leading up to the launch, with the countdown being postponed multiple times. But after so much preparation, it became less stressful.

We anticipate many possibilities while in the simulator on the ground. It is important to note that the simulations are extremely close to real the conditions experienced in space. The instruments are the same, the controls are identical as well. For example, the fact that I did not discover all of this when I boarded the shuttle helped to reduce the stress.

During the engine ignition, a piece of metal detached from engine three (on the right) and struck the internal surface of the nozzle, tearing off three cooling tubes containing hydrogen. A short circuit partially disabled the right engine, which was compensated by the backup system increasing the hydrogen flow. This caused a rise in temperature, ultimately leading to the premature shutdown of all three shuttle engines. We came dangerously close to a disaster! An engineer on the ground was later rewarded for their exceptional work on this mission !

What is your perspective on the emergence of new players in the space industry, such as SpaceX or Blue Origin ?

The Columbus shuttle

Elon Musk has succeeded where traditional space agencies paused their efforts. Personally, I believe it is a winning bet, both financially and technically. He has instilled an exceptional work rhythm. We can say that the U.S. has regained its space independence. It is truly a win-win situation, as every flight is meticulously analyzed and scrutinized to learn from any dysfunctions and implement improvements for the next mission.

The great strength of SpaceX, and its founder Elon Musk, lies in his ability to unite people around his vision and establish an exceptional work rhythm. We can confidently say that the U.S. has regained its space independence. There's been a lot of talk about space tourism, but it remains very expensive, with ticket prices reaching around 50 million euros during the last Polaris mission. However, I am convinced that humanity will reach Mars, not necessarily on Elon Musk's timeline, but we will get there, that is certain.

You're the one who recruited Thomas Pesquet, how does it feel to see his success today, does it make you proud ?

Recruiting an astronaut is a long and rigorous process requiring exceptional skills and intensive preparation. Thomas Pesquet is undoubtedly the most well-known French astronaut of his generation. He has played a pivotal role in making space careers popular and has significantly contributed to making space exploration more accessible through his communication efforts. Of course, it is a great source of pride for me to be the one who recruited him.

It's important to note that, initially, there were over 8,400 candidates in the first phase of recruitment, and in the end, only six were selected. The second phase, which was more recent, saw no fewer than 20,000 applications.

It's a point of pride for me, as I see in Thomas a man who sets an example for the younger generation. I am confident that future selection campaigns will see similar success.

There is also pride in recruiting Sophie Adenot, who is set to make her first space flight in 2026.

Thomas Pesquet

Is writing books a duty to preserve memory for future generations, or a personal need ?

Both !

I believe it's my duty to leave a mark for future generations. They will be able to discover, in an astonishing way, what we managed to accomplish.

These books are a way to mark history, both technically and descriptively. It is important to have written records for the centuries to come. In a way, it's about staying in history.

The title "A Coffee in Space" refers to the fact that the first thing I was offered in space was a cup of coffee. You see, as an astronaut, there is the operational side where you perform tasks, and then there is the transmission side where you explain things.

I have transitioned into that second phase now.

Looking back, what would you say to your younger self if you could meet them today ?

Jean-Loup Chretien and Michel Tognini

If I could go back in time and meet my younger self, I would tell this child to believe in their dreams and never give up too soon! You are capable.

When I was younger, I was not great at school, I have to admit… But in middle school, I had a math teacher who helped me go from last in the class to first. What used to be a difficult subject became an easy game. Those encounters change lives !

If a young person wants to become a teacher, a mathematician, or even a baker, it does not matter what profession they wish to pursue, they need to give their all to succeed and hold on tight! Every job deserves 100% effort to truly thrive.

That teacher inspired me to study. In fact, I work with teachers now, and I can see that we have an extraordinary teaching staff.

Some children may feel lost, but they manage to persevere thanks to education. Everyone should have that magical encounter with a teacher who lifts them up.

Thank you for taking the time to speak with us. Would you like to share a final thought to conclude this interview ?

I will conclude this interview by sharing two quotes that I truly love :

« The Earth is the cradle of humanity, but mankind cannot stay in the cradle forever » Konstantin Tsiolkovski.

« As for the future, your task is not to foresee it, but to enable it » Antoine de Saint-Exupéry.

Interviews

With the game-changers shaping the future of IT & Cybersecurity

Once again, our interview section returns: six new profiles, for six new stories !

SOUFIANE TAHIRI

Head of Offensive Security - Peaksys

Hello Soufiane, can you tell us a bit more about yourself ?

"Hello Arnaud !

I'm Soufiane, tech enthusiast, but I've always had a strong interest in nature, animals, drawing, woodworking, and philosophical questions... none of which have much to do with IT."

What was your career path ?

"I'm not sure it's a typical path, but let's just say my studies didn't necessarily contribute much to my professional career. I was lucky enough to 'virtually' meet people who were already interested in cybersecurity well before it became trendy (around 2003).

I learned a lot with them, from reverse engineering to penetration testing (a term that didn't even exist back then), as well as development.

This hands-on experience eventually led to a job when paying bills became more important than learning how to reverse engineer a malware...

I had a rather chaotic academic journey, but for what it's worth, I did study a bit of economics at university."

What are your daily tasks and responsibilities ?

"Today, I'm responsible for a small team of pentesters. My daily work mainly involves assigning missions and overseeing penetration tests.

I also keep up with more or less active threat monitoring, do some research and development, and stay focused on offensive strategies."

What does a typical day look like for you ?

"A typical day is probably like anyone else's, I imagine, answering emails, attending meetings, and trying to find as many ways as possible to exploit an information system or an application before the "bad guys" do."

What do you like/dislike about your job ?

"What I enjoy about my job is the constant challenge. No matter how good you think you are, you often end up not understanding what's happening on your screen.

What I dislike about it is that it has become a job, and sometimes, the job kills the passion."

A final word ?

"No matter how skilled we think we are, there is always someone better. This field is built on sharing and humility, never forget that: sharing and humility."

HUSSEIN AISSAOUI

Cybersecurity Architect - SFR Business

Hello Hussein, many people know you, but can you tell us who you are ?

"Hello Arnaud !

I am a Cyber Security architect with a 360° approach to Cyber. I don't limit myself to specific topics or areas."

What was your career path ?

"I originally started as an expert in Microsoft Active Directory technologies and Exchange messaging, and I was a passionate basketball player, which made me discover and appreciate challenges and management.

Over time, as I took on more complex and interesting projects, I gradually added the Security role, which naturally evolved into Cybersecurity at large."

What are your main responsibilities ?

"On a daily basis, my mission is to share my cyber expertise across both standard and more confidential areas. And to build the best possible defense against cyber threats that evolve day by day.

Whether it's technological advancements or global conflicts which constantly generate new threats
"

What does a typical day look like for you ?

"It doesn't really exist. I consume a lot of cyber literature (a lot!), I continuously discover and work on new developments, always staying on top of emerging threats in all their forms.

So, my typical day consists of a lot of CYBER LIVE."

What do you like/dislike about your job ?

"What I love about my work is everything... truly! Specifically, I enjoy anything that's innovative, bringing fresh perspectives and new methods to get more secured systems.

AI is a tremendous opportunity to take cybersecurity (both attack and defense) to the next level.

As for what I dislike... it's simply the fact that there are only 24 hours in a day ! "

A final word ?

"We're only at the beginning of the crossroad between cybersecurity and AI... and this promises fantastic developments ahead.

The key question is, will we benefit from it, or will we suffer the consequences ? It's up to us to ensure that cybersecurity works for us and our businesses."

MARC-ANTOINE LEDIEU

Lawyer, Legal CISO & Speaker

Hello Marc-Antoine, could you tell us a bit about yourself in a few words ?

"Hello Arnaud, I'm Marc-Antoine LEDIEU, a lawyer at the Paris Bar for nearly thirty years. Since 1997, I've been drafting IT contracts to regulate the business of digital professionals. Since 2014, I've been explaining laws and technical concepts in a simplified manner, particularly through accessible comic strips available on my website.

In 2013, I shifted my focus to cybersecurity. In 2017, the WannaCry and NotPetia malware attacks led to the introduction of special "cybersecurity" annexes in B2B IT contracts. The DORA and NIS2 regulations (December 2022) and LPM2023 are the key texts relating to mandatory cybersecurity rules, which are keeping us quite busy at the moment...
"

What was your background before that ?

"My journey began with studies in business law and contract law.

In order to improve my understanding of the technical aspects, I self-taught myself digital technologies, blockchain, and cybersecurity.

In 2021, I obtained the ISO 27001 Lead Auditor certification. "

What are your main responsibilities ?

"I rarely plead cases. I mainly focus on deploying DORA and NIS2 projects.
My work on communication through comics (on my website and LinkedIn profile) takes up quite a bit of my time, along with staying updated on technical and legal news.

I also teach cyber law and participate in 'hacker' conferences. As a Legal CISO, I support CISOs in the legal aspects of their work (regulations, technical standards, case law, etc.)."

What does a typical day look like for you ?

"My days start with at least an hour of documentation (official journals, online news, etc.) in the digital world.

Then, I focus on delivering services to my clients (advice, negotiations, etc.)"

What do you like/dislike about your job ?

"What I enjoy about my job is helping companies implement data security measures. The downside: companies always trying to negotiate my rates (because cybersecurity is easy, it doesn't bring in much, but it's always too expensive...)"

Do you have a final word you would like to share with us ?

"Cybersecurity legislation isn't a bad thing, but it is necessary! Our companies and businesses are entirely dependent on digital systems.

However, none of our information systems or software were designed with cybersecurity concepts in mind."

DAMIEN BANCAL

Journalist for ZATAZ & Cybersecurity Researcher

Hello Damien, who are you ?

"My name is Damien Bancal. I'm 52 years old, and I am a journalist and researcher combating cybercrime.

I'm the founder of the blog ZATAZ.COM and the company VeilleZATAZ.com. I am passionate about discovery and knowledge-sharing. Eager to see what I'll learn tomorrow."

Can you tell us more about your career path ?

"I always wanted to become a journalist, even from a very young age. I loved finding answers to questions, or adding more questions to those answers. At 14, I met my first hacker, a 'phreaker' who specialized in telecom hacking. I ended up writing about it.
At the time, I already had a blog on an Amstrad CPC, and yes, back then, diskettes only held 128 kilobytes of data!
Later, I pursued studies in communication, but I was already working for publications focused on high-tech, video games, and even general-interest news.
It was during this period in Lille (France) that I met Eric, who was a webmaster at the time and is now a master of cybersecurity. He encouraged me to bring my project, ZATAZ, to life on the web, the real web, not just a blog. And that's how ZATAZ.COM was born.
As we approached the 2000s, ZATAZ had already been thriving for 10 years.
As a passionate communicator, I joined the communications teams of two municipalities in northern France, eventually becoming the head of communications for one of them.
In 2019, a Quebec-based company contacted me and I became their Head of Cyber Intelligence, based in Montreal. Unfortunately, the COVID-19 pandemic disrupted this project. I spent nine months away from my family
"

What are your main responsibilities ?

"It's not easy to explain without revealing professional secrets. We work in an environment where controlling social engineering is crucial.
So, I'd say my tasks are split between research and investigations for the monitoring service and the blog. At SVZ, we use about twenty fully internal tools, fourteen of which I developed myself.
Also, a significant part of my work involves communication and networking: connecting with partners, readers, prospects, and even hackers."

What do you like/dislike about your job ?

"I am incredibly lucky to work in a field I've always dreamed of. On top of this, I've been able to tailor it with the options that matter most to me.
But luck doesn't come without hard work, meaningful connections, and constant motivation.
The only downside? There are only 24 hours in a day.
"

What does a typical day look like for you ?

"Varied is an understatement, I don't have a typical day.
Take Thursdays, for example: I'm up at 5.00 am, followed by a TV/radio show from 9.00 pm to 12.00 pm. The commute to and from the studio allows me to gather overnight news updates for ZATAZ.COM.

Back at the office, from noon to 2.00 pm, it's all about handling SVZ relations, press inquiries, and similar tasks. At 2.00 pm, my phone and other connected devices go into a 'no-connect' zone so I'm unreachable. From 2.00 pm to 8.00 pm, I focus on various projects. By 8.00 pm, it's family time.

At midnight, I pick up where I left off, provided there are no unexpected surprises. But let's be honest, a life without surprises wouldn't be much fun! :)"

Do you have a final word you would like to share with us ?

" I've always been told that my curiosity was a bad habit, but believe me, my flaw is a charming curiosity."

JULIEN METAYER

Pentester - Redteamer - OSINT Expert - Mentor

Hello Julien, tell us : who are you ?

"Hi Arnaud !

I'm 47 years old, originally from the development world. I've also managed web infrastructures, but about six years ago, I returned to hacking, pentesting, and red teaming. Beyond that, I organize investigations in companies and also do some consulting with the French Ministry of Interior's Cyber Command (COMCYBER-MI).

Additionally, I'm a mentor at Guardia Cybersecurity School. As for the rest of my free time, I take part in various conferences. I am also the founder of the ozint.eu website, which became osintopia.

Can you explain your background ?

" 25 years ago, I completed a Master's in Applied Computer Methods for Business Management (MIAGE).

Like many of us in our field, I'm self-taught and love to learn new things. I also attended M2i Formation school to formally validate some of the knowledge I had acquired.

By the way, I want to give a shout-out to one of my instructors, Jordan Douliez, who's truly a gem !"

Are there things you like or dislike about your job ?

"What I genuinely enjoy about my work is the variety it offers, I never get bored or tired of it. The human aspect is also a big source of satisfaction, as well as the ability to work remotely. Essentially, what I love most is the flexible management of my work schedule.

What I dislike, however, is the lack of long-term client loyalty, which means I have to network quite a bit. Additionally, being independent isn't always an advantage, as there's a lot of competition with larger companies which, unfortunately, doesn't always guarantee quality.
"

What are your main responsibilities ?

"Generally, my tasks revolve around web penetration testing.

I also organize monitoring sessions and networking events, but this varies depending on the time of year. For example, in October and November, I often attend conferences (either as a speaker or classic participant) .

I'm lucky to be freelance, which gives me a great deal of freedom to manage my schedule.
"

What does a typical day look like for you ?

"I always start my mornings with two hours of research and some cyber monitoring, and working remotely gives me the freedom to set my own schedule. After that, I dive into the various tasks I mentioned earlier. This setup also allows me to travel a lot, and I enjoy this freedom. In the end, I'm doing what I love.

I'd rather focus on what truly excites me now, even if it means earning less income."

Julien, any final word you would like to share with us ?

"In OSINT, ego battles are way too present and it's unfortunate...

It's essential to stay aware of what's happening on social networks. It's important to raise awareness among younger generations about key topics like ethics, photo sharing guidelines, and more…"

FRANCK CECILE

Cybersecurity Compliance Officer

Hello Franck, can you tell me more about yourself ?

"Like many of us, I'm passionate, not so much about cybersecurity itself, but about new technologies, the changes they bring to our daily lives, the risks, and the potential misuses we can make of them...

Both in terms of purely technical aspects (although, let's be honest, I'm past the age of tinkering with Kali), and in areas that require a bit of perspective... Organizational challenges, geopolitical risks, structuring a digital/cybersecurity department to face business challenges..."

Can you tell me a bit more about your background ?

" IT Technician, Network and Security Engineer and Architect, Network Consultant, Datacenter, and then Cybersecurity. And now, Cybersecurity Compliance Officer.

I've held quite a few roles and missions, both with end clients and in services, management, or pure consulting, across various industries, including IT & OT. But ultimately, I've always worked in security. Initially, my focus was more operational, and now it's clearly more organizational.
"

What are your daily tasks ?

" Governance and compliance. I won't say more, but although this field is often seen as 'boring,' there's actually plenty of room for excitement in GRC (Governance, Risk, and Compliance) tasks "

What does a typical day look like for you ?

"Excel and PowerPoint are my best friends, haha!

More seriously, I moved away from technical roles to focus on leadership, coordination and organization. It sounds like a lot of 'buzzwords' to our operational colleagues and I get it. GRC work is rarely “tangible”.

However, it’s essential and both complement each other.

This means a lot of communication, some occasional “lobbying”, and above all, being able to take a step back to gain perspective on complex issues."

Are there things you like or dislike about your job ?

"I often find myself caught between the operational and organizational worlds, which I believe is a key challenge for anyone working in cybersecurity. While these two areas are complementary, they often fail to understand each other and, at times, they can clash.

On the organizational side, the results of our work can be hard to see, as they’re often more abstract.

Outcomes on the operational side are much more concrete, but I also know how frustrating it can be when a strategy doesn’t align with what you want. Unfortunately, these are the challenges we have to deal with."

Thanks, Franck, any final thoughts ?

"AI will save us (or maybe not)."

Starlink, A prime target ?

The conflict between Ukraine and Russia is a cyber war that goes beyond anything we have ever witnessed before.

Nicole Petrucci
Chief of Space Delta 3 in the United States Space Force

Two days after the invasion, Starlink services were activated in Ukraine to provide high-speed internet access to the Ukrainian population, government, and military.

On March 5, 2022, Elon Musk announced that SpaceX resources were being "prioritized for cyber defense and countering signal jamming", suggesting a potentially high number of cyberattacks.

Due to the intensity of Russian electronic attacks against Starlink, SpaceX also had to remotely update the software on its user terminals.

The pro-Ukrainian hacker group Cybersec announced it would retaliate against these attacks. By May 2024, Starlink had over 3 million customers, a significant portion of which were in Ukraine.

Analysis of the social media accounts of threat perpetrators reveals that Starlink is frequently mentioned by hacktivists.

Pro-Russian groups often share information about the company, highlighting the Russian military's ability to purchase used terminals for their own use or to track terminals used by Ukrainian armed forces. Given the importance of Starlink for Ukraine's military operations


Starlink Modem

and its civilian population's ability to access the internet, one might assume that the number of cyberattacks against Starlink would be very high. Surprisingly, the data collected shows only a limited number of operations targeting Starlink.

Killnet carried out two DDoS attacks against Starlink's official website and authentication portal. Sandworm infiltrated Ukrainian Android tablets, which were used by Ukrainian soldiers and connected to Starlink, to gather information about the satellite constellation.

What stands out is that these three incidents received significant media attention compared to many other attacks on the space sector, highlighting Starlink's high value as a target for pro-Russian cybercriminals.

Hacktivist groups on both sides are interested in targeting Starlink with cyber operations due to its potential for significant impact on the front lines.

For example, a spokesperson for the Ukrainian military stated that Russia was using Starlink on the battlefield, and that if the group was "able to disrupt communications near Russian administrative points, they won't be able to see their drone data from the front.

However, the Ukrainian military has never claimed responsibility for any electronic or cyberattacks against Starlink in its public communications.

We can assume that the military would ultimately see an attack against Starlink as a double-edged sword, where both Ukraine and Russia could be affected.
.

Starlink Satellites

Starlink supporting or opposing Ukraine ?

It's not as simple …

In April 2024, Dmitry Kuzyakin, CEO of the Russian Center for Integrated Unmanned Solutions, which produces and trains military drone operators for first-person view (FPV) drones, accused the Ukrainian armed forces of hacking Starlink terminals to bypass territorial restrictions.

SpaceX had blocked Ukrainian armed forces' access to Starlink in areas such as Crimea and for specific operations, such as drone strikes.

These accusations stem from the claim that Russia successfully captured and dissected a Ukrainian military drone, 'Baba Yaga,' which was equipped with a Starlink antenna.

This led them to discover that significant modifications had been made to the terminal and software to remove territorial restrictions and paywalls, enabling Starlink to be used beyond its intended limits.

Kuzyakin stated that a Raspberry Pi (a small single-board computer) was likely used to implement these changes. He claimed that such modifications would be impossible without insider information, either directly provided by SpaceX to support the Ukrainian Armed Forces, or coming from a data leak containing sensitive information about Starlink.

However, it is impossible to verify Kuzyakin's claims.

Space Data Centers: Are We Ready Yet ?

The explosion of data and the rise of artificial intelligence are pushing digital players to rethink their infrastructures. Faced with the limitations of terrestrial data centers in terms of energy and environmental impact, a radical solution is emerging: space-based data centers.

While the challenges are significant, the potential is enormous. Space data centers could revolutionize high-performance computing by offering unmatched processing and storage capacities. They could also play a key role in the development of new applications, such as artificial intelligence, and in advancing scientific research.

Several companies such as HPE, Thales Alenia Space, and Axiom Space, are already exploring this topic. Each of them with projects that have their own advantages and challenges.

Thales conducted a feasibility study called ASCEND. It aimed to compare the environmental impacts of orbital data centers with those of terrestrial ones.

The study also intended to evaluate the technological feasibility of developing, deploying, and operating them in orbit.

To significantly reduce CO2 emissions from the storage and processing of digital data, the study's results estimate that such space-based infrastructures would require the development of a launcher with ten times lower emissions across its entire lifecycle. Additionally, the water consumption required for their cooling would be eliminated from the process, which would be a major advantage.

Modular space infrastructures would be assembled in orbit using robotic technologies, which will be demonstrated in the European Commission's EROSS IOD project, led by Thales Alenia Space, with the first demonstration expected by 2026. Meanwhile, HPE and Axiom are rethinking the traditional data center and see a promising future for it in the medium term.

Low Earth orbit (LEO) data centers could help save land on Earth, reduce electricity costs through solar power technology,

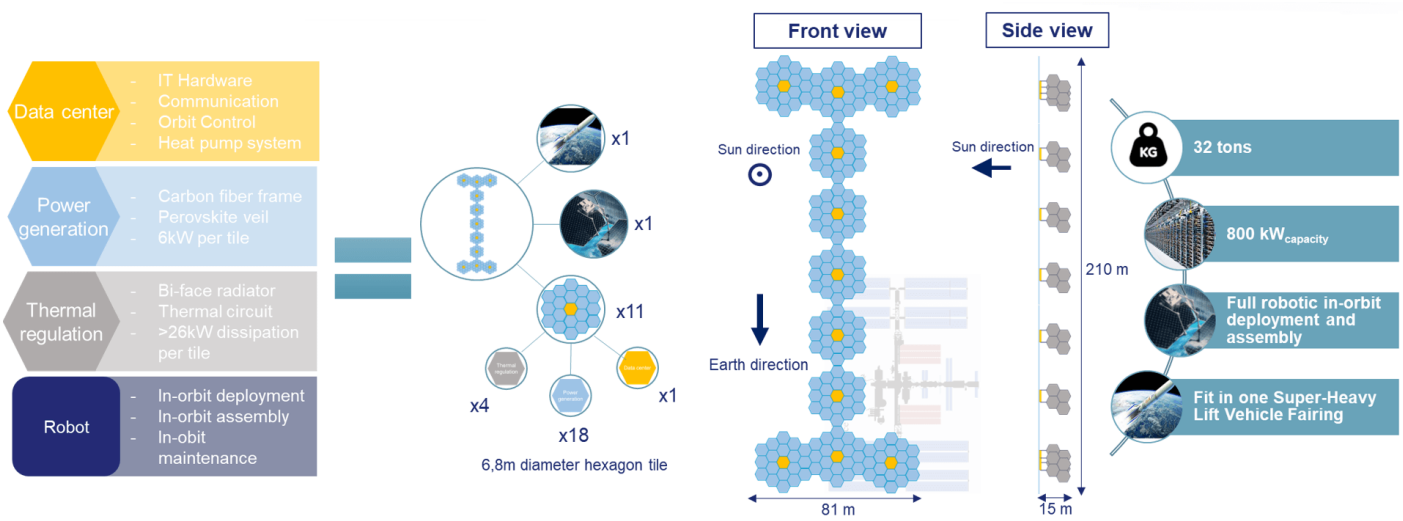
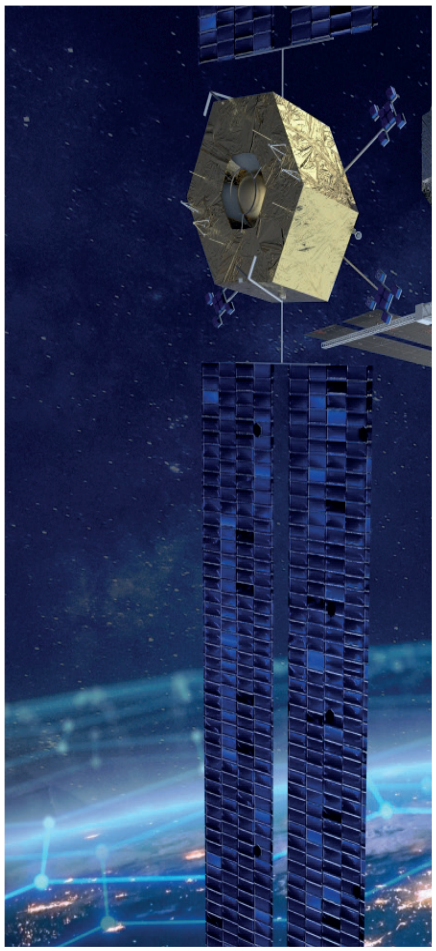
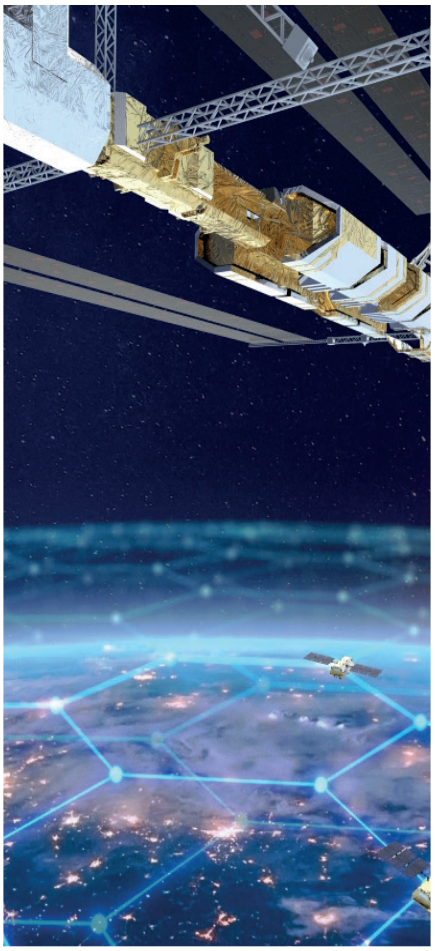
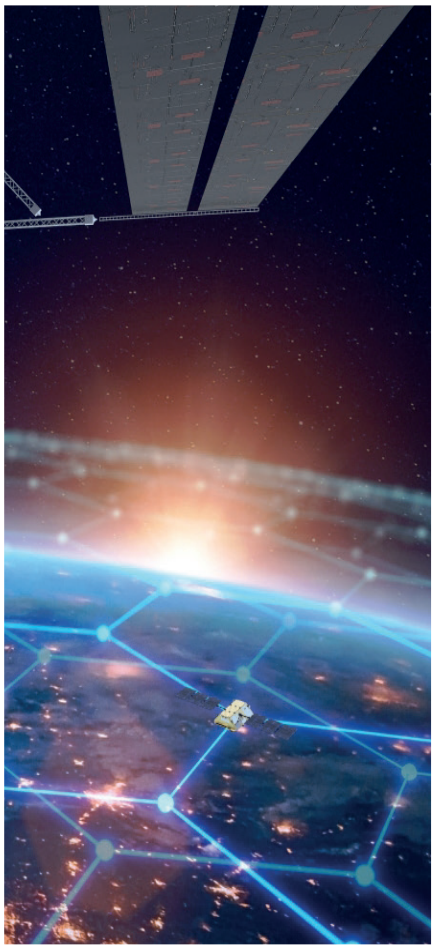


Diagram illustrating planned operations with ASCEND Cloud In Space







and even lower data latency. In space, solar energy and batteries would provide all the power, thus reducing operating costs.

A low-orbit data center, completing a full orbit of Earth every 90 minutes, would be exposed to sunlight for about 45 minutes with each rotation. During the rest of the time, the data center would operate using batteries connected to its solar panels.

Cooling solutions are also a concern. There can be a temperature difference of several hundred of degrees between sunlight and the darkness caused by the Earth. In space, traditional cooling systems lose their effectiveness because convection does not occur in microgravity.

Ammonia-based radiators are used to cool space computers, similar to those aboard the International Space Station (ISS). However, several issues remain unresolved. For example, orbital launcher models will need to be adapted. Maintenance and end-of-life management also still need to be clarified, as well as the impact of solar radiation on the deployed installations.

The end-of-life management of space data centers also remains to be clarified.

ASCEND
Cloud in space

Are We Ready to Live on the Moon ?

with Jamy Gourmaud

In 2026, NASA and SpaceX, Elon Musk's company, promise to take us back to the Moon. However, the journey began earlier in 2022, when the Earth's satellite witnessed the launch of the Artemis 1 rocket.

The mission's goal was to orbit the Moon and return to Earth. No humans were aboard, instead, mannequins had the unique privilege to "see" the Moon up close.

The next significant milestone will be Artemis 2, which will replace the mannequins with four astronauts aboard the Orion spacecraft.

This mission is scheduled to launch in April 2026. The most remarkable step, however, will be the third Artemis mission. This mission's goal is to land astronauts at the Moon's south pole for a six-day stay.

The goal of these missions is to explore the feasibility of establishing a future lunar launch base for journeys to the Red Planet: Mars!

However, this will not be possible until 2040, or perhaps even 2050. NASA wants to create a base camp on the Moon, serving as a stepping stone before sending astronauts to Mars.

Yet, several challenges are associated with life on the Moon :

AIR

Earth has an atmosphere, a delicate layer of air allowing us to breathe. The Moon, however, has no atmosphere. To transport some air to the moon, a spacecraft would need to travel an immense distance of up to 384,400 km, the farthest point when the Moon is at its most distant from Earth. For comparison, the International Space Station orbits just 400 km above our planet.

NASA scientists may have found THE solution in Moon dust, which contains oxygen.

They developed a laser capable of reaching 1,600°C to melt the dust, primarily composed of regolith and extract the oxygen it holds.

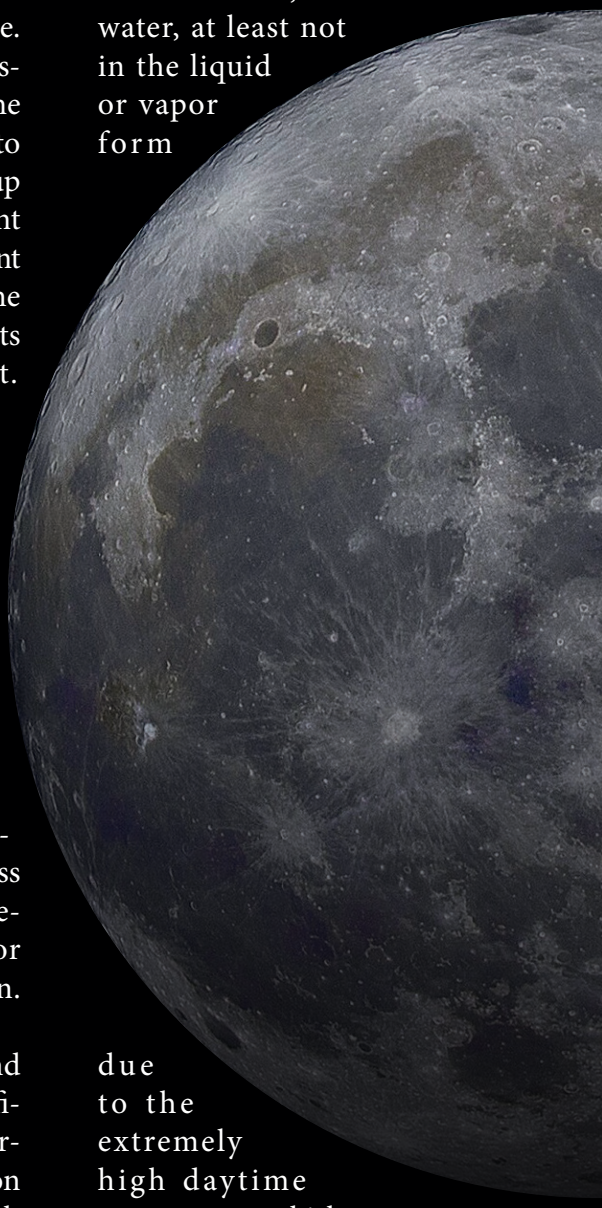
Tests conducted in a vacuum environment, mimicking the airless conditions of the Moon. The results are already promising for use in a future Artemis mission.

The Moon is also rich in silica and aluminum, which contain significant amounts of oxygen. According to some scientists, the Moon could potentially hold enough oxygen to sustain 8 billion people for approximately 100,000 years.

The only remaining challenge would be to supply nitrogen, completing the necessary elements to recreate breathable air on the Moon. For reference, air consists of 21% oxygen, 78% nitrogen, and 1% trace gases.

WATER

On the Moon, there is no water, at least not in the liquid or vapor form due to the extremely high daytime temperatures, which can reach around 150°C. However, at the lunar south pole, scientists have discovered numerous ice deposits hidden in craters shielded from sunlight and protected beneath a thick layer of regolith. To harness this resource, the Americans have developed an innovative extraction module called the Rocket M.



This module can pulverize rock and extract ice, transforming it into water vapor in just 5 to 10 minutes. According to its creators, this robot could process up to a dozen craters daily, collecting a total of 426 tons of water annually. A portion of this water would be used as fuel for SpaceX rocket engines, while the remainder would support astronauts' needs.

However, this accessible water represents only a small fraction of what the Moon may hold. Chinese researchers claim that the Moon harbors a massive reservoir—not underground lakes, but tiny glass beads formed by asteroid impacts. These beads are estimated to contain the equivalent of 270 billion cubic meters of water. Yet, accessing and extracting this water remains a significant challenge. So far, no such efforts have been successful.

FOOD

Americans achieved a significant milestone by creating a soil similar to regolith, the Moon's dust. They experimented by planting chickpea seeds, and after a few days, some began to sprout, with some even reaching maturity.

This suggests that, in theory, it is possible to grow something on the Moon. Australian researchers are planning to send tomato and carrot seeds in a module to the Moon in 2025 to conduct a similar experiment.

Inside this module, once landed on the Moon, a small robot will plant these seeds in the soil and cultivate them in greenhouses to protect them from the extreme temperatures of the lunar environment

ENERGY

The Sun will allow astronauts to generate energy using solar panels. However, many panels will be needed to provide enough electricity to power computers, workshops, machines, lighting, heating, and even vehicles during the missions.

The American project Blue Alchemist aims to manufacture panels using lunar regolith, which would have the advantage of being produced on-site.

REGOLITH

It covers the entire surface of the Moon with a thickness ranging from three to twenty meters. This dust is composed of microscopic grains, with an average size of 19 microns, which is half the size of a human hair. They are so thin that they stick to astronauts' suits, infiltrate the smallest components of machinery and they can enter the body through the respiratory system.

In 1969, the first men to set foot on the Moon reported the issue. The dust emitted a smell similar to gunpowder, causing sneezing and severe coughing fits. In 2018, a team of British researchers demonstrated that lunar dust, which is abrasive, can be potentially harmful to health. Breathing lunar dust particles is as damaging to the lungs as working in a coal mine without protection.

Therefore, NASA, along with private companies, is working on new space suits which would prevent these particles from infiltrating. However, no prototype is ready yet .

CREDITS

Editor-in-Chief : Arnaud LEROY
Graphic Design : Arnaud LEROY
English Translation : Maëva ASTORGA
Magazine Mentor : Guillaume Poupard

We would like to thank everyone who contributed to this issue.

January/March 2025