Atlantic Council

GCSP Geneva Centre for Security Policy

Cyber 9/12 Strategy Challenge

Intelligence Report I

INSTRUCTIONS

Please read these instructions carefully. They have changed from previous years.

Your team will take on the role of experienced policy advisers, part of a hypothetical cybersecurity task force, preparing to brief the European Space Agency (ESA). This packet contains fictional information on the background and current situation involving a major cyber incident affecting EU and Switzerland interests. The incident notionally takes place throughout 2025. The scenario presents a fictional account of political developments and public reporting surrounding the cyber incident.

The ESA needs information on the full range of response options available regarding this incident. Your team has been tasked with developing an appropriate course of action for recommending to the ESA.

You are to consider as facts the following pages for formulating your response.

You will use the fictional scenario material presented to perform three tasks:

Written Situation Assessment and Policy Brief: Your first task is to write an analytical 'policy brief' that provides a concise assessment of the situation, addresses potential impacts and risks, and discusses the implications of the cyber incident. Describe policy considerations for different potential state and non-state actors. Be clear regarding the advantages and disadvantages of various policy options and explore the course of action you are recommending in depth. The

length of the 'policy brief' is limited to **two single-sided pages**. Your judges **will not** see this Written Brief before the competition. The Written Brief will be graded by members of the Cyber 9/12 Scenario Team.

Written briefs are due no later than **Tuesday, March 25th, 2025** at **17:00 CET (Central European Time)**. Please submit your written policy brief as a .docx or .pdf to cyber-competition@gcsp.ch Please note that your **team name must** be included in the title of the submission file name, **as well as** in the subject of the email. Late submissions will be assessed a penalty.

Oral Policy Brief (Day 1): For the first day of the competition, prepare a ten-minute oral presentation outlining your impact and risk assessment, as well as your suggested course of action. You will present to a panel of judges playing the role of the ESA.

Decision Document (Day 1): Teams will also be required to submit a 'decision document' accompanying their oral presentation at the beginning of the competition round. The 'decision document' will be a maximum of **one single-sided page** in length, outlining the team's response options, decision process, and recommendations. The teams should note that the document is not intended to summarize every detail of the recommendations, but to help the judges follow the oral presentation, and the judges will be given only 2 minutes to read it before the presentation begins. The document should be written with the goal of assisting busy senior officials to quickly grasp your team's recommendations and analysis. Please submit your Decision Document as a .docx or .pdf to cyber-competition@gcsp.ch Please note that your **team name must** be included in the title of the submission file name, **as well as** in the subject of the email. Late submissions will be assessed a penalty. Teams who do not have a Decision Document accompanying their Oral Briefing will be assessed a penalty.

Keep these tips in mind as you are reading and considering your policy response alternatives:

- *Analyze the issues.* The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of potentially conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.
- *Engage the scenario.* Believe that the universe we have created is plausible and that the events that happen in it are realistic. Nevertheless, remember to think critically about the intelligence you have been provided and its provenance.
- *Think multi-dimensionally.* When analyzing the scenario, remember to consider implications for other organizations and domains (e.g. private sector, military, law enforcement, different levels of government, diplomatic) and incorporate these insights along with cybersecurity.
- *Consider who you are, and who you're briefing.* You are experienced cyber policy professionals briefing the European Space Agency (ESA). As such, you should be ready

to answer questions on agency responsibility, provide justifications for your recommendations, and have potential alternatives ready.

- *Be creative.* Cyber policy is an evolving discourse, and there is no single correct course of action to the scenario information provided. There are many ideas to experiment with in responding to the crisis.
- *Don't fight the scenario*. Unless stated otherwise, assume all inter-state relations, policies, and treaties have remained the same as they were in March 2025. Explore the implications of that information, not the plausibility.

Given the unclear nature of the threat, the ESA requests that your team prepare a concise assessment of the ongoing situation and reporting. Your assessment should include:

- How or where the relevant systems could be vulnerable to exploit, and what steps can be made to mitigate these vulnerabilities;
- An assessment of potential risks and impacts to consider if the vulnerabilities are successfully exploited;
- Responses (minimum 2) the ESA can or should consider addressing these vulnerabilities, taking into account the severity and likelihood of the threat; and
- The timeline within which these responses should fall.

To provide this assessment and policy recommendations, you will apply your understanding of the technologies involved, cybersecurity, law, foreign policy, international relations, and security theory to synthesize useful policy measures from limited information. Your recommendation must analyze the possible strengths, weaknesses, opportunities, and threats of your proposed response. In formulating your response, you will be expected to have considered, at a minimum:

- All stakeholders when determining an action or recommendation, including the role of the government and private sector;
- The long and short-term impacts of your recommendation;
- Which agency will be responsible for the action you have recommended;
- Relevant directives, orders, laws, or systems which could be called upon;
- Appropriate recommendations for local vs. federal government;
- Whether you can, or should, attribute the threat; and
- The covert or overt nature of your response.

This message is accompanied by several documents that may assist your team in preparing the assessment and policy brief for the ESA. In an effort to deliver a realistic scenario that is still considerate of our participants' affiliations, we are including some materials that should be treated like classified documents, despite not being formatted as such. These documents will include a disclaimer and are marked below with an asterisk. The document disclaimer will include the intended level of classification of the document for scenario purposes. Please review the documents included below:

- **Tab 1** – EU Intelligence Email Communication
- **Tab 2** – Media Profile Article
- **Tab 3** – O Corporation SatOps Slack Channel
- **Tab 4** – GSP EBook
- **Tab 5** – Preview Blog Post
- **Tab 6** – Space ISAC Forum Post
- **Tab 7** – Internal Emails

Note: To help with your preparation, you have been provided with background information. This information is sufficient to tackle the situation at hand.

Tab 1 – EU Intelligence Email Communication

From: Lew Davis <davis.lew@hq.nato.int>
Sent: Saturday, September 6, 2025, 9:47am
To: EU-IC-List-External
Subject: Intermittent satellite signal outages

TLP AMBER

Several analysts throughout the UK*, EU* and Swiss* intelligence agencies have observed the same intermittent outage events affecting multiple space agencies' satellite communications. The outages began on 05 September 2025 at approximately 0330 GMT, appear to last from two to ten minutes, and interfere with telemetry and control. They do not affect entire constellations, nor do they all occur simultaneously, but the timing appears not to be random, so the investigation is proceeding from the assumption of a software problem or external actions.

We are collecting data from the ground tracking stations through their associated agencies, but the G3 geomagnetic storm that commenced today at approximately 0500 GMT is interfering with some diagnostics. We expect the geomagnetic disruption to abate within ten hours and do not associate it with the outage events that began earlier.

Thus far, we have received corroborating reports from the NATO Space CoE, Eutelsat, ARTES in the UK, and NASA. The ESA's ESOC in Darmstadt is asking for any other data collected by monitoring, from 05 September onwards, to be forwarded to them as soon as possible. Thank you.

Will touch base again if any updates,
Lew

Lew Davis
North Atlantic Treaty Organisation (NATO)
Associate Manager

Tab 2- Media Profile Article

HOME. LATEST. POLITICS. TECH. INFLUENCE. TRENDS.

Conquering the World From Space Imier de L'Étivaz and His Reign of Terroir

September 6, 2025

Vaud, Switzerland - As we settle in for an apéritif at a discreet establishment, Imier de L'Étivaz carelessly stacks his iPhone 16 Pro Max, Google Pixel 9 Pro XL, and his Samsung Galaxy Z Fold6 on his side of the table (perhaps taking up a bit more than his side, but we won't mention it). His gaze travels frequently from the phones to meet my eyes, but then wanders over to the front door, the other diners, and the curated art hanging from the ceiling. His security detail, seated nearby, pretends to look at the menus, but it's pretty clear that the gentlemen don't read French, and might have trouble handling the delicate glassware with their large muscles and beefy hands.

"I can't stay long," he announces. "I'm heading to Brussels tonight, and then Australia in the morning."

L'Étivaz, 47, has been constantly on the move ever since he established his foothold in Switzerland as founder and CEO for O Corporation, the conglomerate that is taking the space industry by storm. O Corporation (O Corp) is best known for its communication satellites that are being launched by the dozens and that promise to transform "the global veil," as he calls it. As of this writing, approximately 15,000 O Corp satellites are in low Earth orbit (LEO), with more planned launches through next year.

If you can't find much backstory to L'Étivaz before, say, 2023, try Googling him under a different name: John Montrey. He will tell you that he's from the Bay Area, but records show that he grew up in Cherry Hills Village, Colorado, before heading farther west to seek his fortune (not that he needed to find one; his hometown is the richest in the state). He was associated with a

number of tech startups — none of which appear to have taken any external funding — and at some point pivoted from FireDactyl.ai to the space industry, hiring all his employees personally and consolidating them in a small town in Nevada before launching (so to speak) the O Corporation, along with a new name for himself.

He hasn't made many friends in the space industry, particularly in Swiss and European circles. Rumors of friction with the European Space Agency (ESA) have not been confirmed, but more than one CNES contractor has reported privately that when de L'Étivaz is mentioned at all in the more established space circles, it's with a mixture of annoyance and amusement. "Even his name is pretentious," said one anonymous source. "Calling himself 'de L'Étivaz' — he's not nobility, and he's certainly not from there." Rather than recruiting more employees from the region, he's still bringing Americans over in large numbers and keeping close tabs on them once they arrive.

However, O Corp has managed to make connections that suit its purposes, such as inking service contracts with satellite networks and ground stations around the globe (many of which are also used by ESA's Estrack). Some examples of space agencies supporting O Corp include ASI (Italy), CNES (France), DLR (Germany), NASA's Deep Space Network (US) and Goddard Space Flight Center and JAXA (Japan). And that's not all: besides the satellite constellations that it owns, the O Corporation also has an uncrewed space rocket program, several manufacturing facilities around the world, and at least five unspecified "laboratories" that we were unable to investigate. There are rumors of a mining operation, but no clues as to what it's actually mining or where.

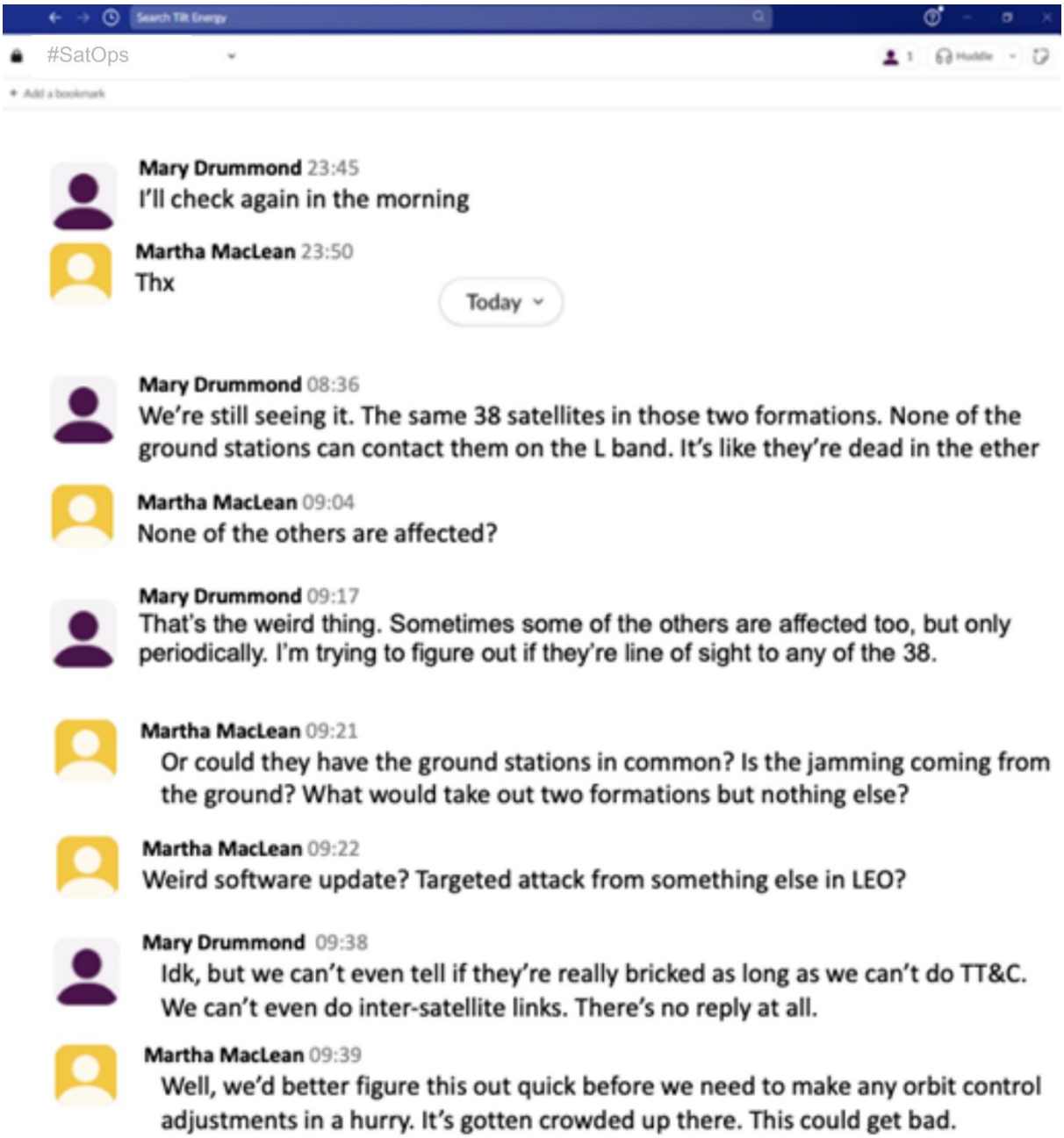
After draining three small glasses of very expensive alcohol, de L'Étivaz finally agrees to answer a few questions. How did he manage to gain the cooperation of the other space agencies? "By making it more painful for them to say no than to say yes." When will O Corp slow down with the satellite launches? "We have no plans to slow down, since we regularly deorbit and replace satellites that are malfunctioning or have used up their power supplies." Is the mining operation used for satellite materials, or are you looking beyond Earth for resources? "That's confidential and proprietary."

And with that, he brusquely shakes hands and collects his bodyguards, who never did get anything to drink. The establishment's staff and the other diners seem to heave a collective sigh of relief as his group walks out the door.

For more content like this from All the Tea please subscribe to our premium list "Piping Hot"

Tab 3 – O Corporation SatOps Slack Channel

Dated: 07 September 2025



Plain Text – Tab 3

Image of the O Corporation Slack channel titled "#satops"

Mary Drummond at 23:45: I'll check again in the morning

Martha MacLean at 23:50: Thx

System message shows "Today"

Mary Drummond at 08:36: We're still seeing it. The same 38 satellites in those two formations. None of the ground stations can contact them on the L band. It's like they're dead in the ether

Martha MacLean at 09:04: None of the others are affected?

Mary Drummond at 09:17: That's the weird thing. Sometimes some of the others are affected too, but only periodically. I'm trying to figure out if they're line of sight to any of the 38.

Martha MacLean at 09:21: Or could they have the ground stations in common? Is the jamming coming from the ground? What would take out two formations but nothing else?

Martha MacLean at 09:22: Weird software update? Targeted attack from something else in LEO?

Mary Drummond at 09:38: idk, but we can't even tell if they're really bricked as long as we can't do TT&C. We can't even do inter-satellite links. There's no reply at all.

Martha MacLean at 09:39: Well, we'd better figure this out quick before we need to make any orbit control adjustments in a hurry. It's gotten crowded up there. This could get bad.

Tab 4- GSP EBook

HOW DOES GPS WORK?

GPS (Global Positioning System) is a network of satellites that continuously transmit signals to receivers on Earth, allowing them to determine precise location, speed, and time.

By measuring the time it takes for signals from multiple satellites to reach a receiver, GPS calculates an exact position using a process called trilateration. This technology is essential for navigation.

Did You Know?
GPS isn't just for Directions!

GPS: The Hidden Backbone of Global Security

You might think GPS is just for getting from Point A to Point B. But in reality, it's one of the most critical technologies keeping the modern world running. Every day, GPS signals guide commercial airliners safely across the sky, help ships navigate vast oceans, and even synchronize global financial transactions.

Beyond navigation, GPS is a foundation for encryption, ensuring secure military communications and protecting sensitive data across the world. It also plays a crucial role in keeping satellites in precise orbits, supporting everything from weather forecasting to internet connectivity.

SATELLITE POSITIONING

AIRPLANE NAVIGATION

MILITARY COMMUNICATIONS

Find Out More on the Next Page

Plain Text – Tab 4

Last Accessed: September 7, 2025

How the World Works - eBook

Chapter 1: Technologies we use daily

Section header: How Does GPS Work?

GPS (Global Positioning System) is a network of satellites that continuously transmit signals to receivers on Earth, allowing them to determine precise location, speed, and time.

By measuring the time it takes for signals from multiple satellites to reach a receiver, GPS calculates an exact position using a process called trilateration. This technology is essential for navigation.

Pop up blurb: Did You Know? GPS isn't just for Directions!

Section header: GPS: The Hidden Backbone of Global Security

You might think GPS is just for getting from Point A to Point B. But in reality, it's one of the most critical technologies keeping the modern world running. Every day, GPS signals guide commercial airliners safely across the sky, help ships navigate vast oceans, and even synchronize global financial transactions.

Beyond navigation, GPS is a foundation for encryption, ensuring secure military communications and protecting sensitive data across the world. It also plays a crucial role in keeping satellites in precise orbits, supporting everything from weather forecasting to internet connectivity.

Satellite positioning, Airplane navigation, Military communications

Find Out More on the Next Page (end of image)

Tab 5 – Preview Blog Post

STRATEGIC STUDIES INSTITUTE
United States Army War College

Published - September 7, 2025

The Role of European Satellite Systems in Modern Warfare

The increasing reliance on low-Earth orbit (LEO) satellite networks for military applications has transformed modern warfare, redefining the battlefield in both conventional and asymmetric conflicts. As demonstrated in recent conflicts, including Ukraine's* defense efforts, access to commercial and government-operated satellite constellations has become a decisive factor in military strategy. This report examines the strategic significance of European satellite networks, their vulnerabilities, and the growing risks posed by cyber and electronic warfare against these assets.

Executive Summary

Since the early 2020s, European satellite systems have played a pivotal role in military operations, serving as command-and-control enablers, reconnaissance platforms, and secure communication nodes. The strategic importance of Galileo (GNSS), Eutelsat, and other European-based satellite constellations has extended beyond traditional military applications to become a critical asset for allied forces, intelligence-sharing, and encrypted battlefield coordination. Electronic warfare (EW), cyber intrusions, and satellite jamming techniques are being actively deployed to disrupt military communications, disable reconnaissance capabilities, and manipulate GPS-dependent encryption systems. As satellite technology becomes more accessible, non-state actors, cybercriminal organizations, and hacktivist groups are also beginning to target commercial and military satellites, raising concerns about the security and governance of space-based infrastructure.

Key Findings

1. European Satellite Networks as Military Multipliers
    - The Galileo GNSS constellation has become a backbone of secure military navigation, synchronization, and encrypted communications.
    - Commercial providers such as Eutelsat and SES have increasingly been contracted to provide high-speed battlefield connectivity and secure satellite communications for NATO operations.
2. Emerging Threats: Cyber and Electronic Warfare on Satellites
    - Cyberattacks against commercial satellite operators have demonstrated the growing vulnerability of space-based assets to both state and non-state adversaries.

   - The use of uplink jamming, spoofing, and malware injections can severely disrupt critical military operations reliant on space-based communications.
   - The rise of privately owned satellite constellations introduces an uncertain regulatory landscape, where commercial interests and national security priorities may be in direct conflict.
3. Lessons from Ukraine's Use of Satellite Systems in Modern Warfare
   - The Ukraine-Russia* conflict highlighted the importance of commercial LEO satellite networks in maintaining battlefield communication even in GPS-denied environments.
   - Distributed satellite architecture proved more resilient than traditional geostationary military satellites, as adversaries struggled to permanently disrupt operational capabilities.
4. Potential Implications of Satellite Jamming in Europe
   - Historical reporting of intermittent outages affecting European satellite networks suggest that hostile actors may be testing interference tactics.
   - If military-grade jamming were deployed on a wider scale, it could compromise battlefield situational awareness, disrupt encrypted command channels, and interfere with NATO operations.

Policy Considerations

- Enhanced Cybersecurity Measures for Commercial Satellite Operators
  - Mandatory cyber resilience standards for private satellite providers that support military operations.
  - Improved coordination between NATO, the EU, and commercial operators to prevent, detect, and mitigate cyber and electronic threats.
- Development of Counter-Jamming and Signal Protection Technologies
  - Investment in anti-jamming technology, hardened encryption protocols, and redundancy in satellite communications infrastructure.
  - Exploration of machine learning-based anomaly detection to rapidly identify and neutralize space-based threats.
- International Legal Framework for Space-Based Conflicts
  - The Outer Space Treaty (OST) and UN Resolutions do not currently provide a clear framework for military responses to satellite interference and cyber intrusions.
  - NATO and EU member states must establish clearer protocols for retaliation and defensive measures in the event of an attack on space assets.

Conclusion

European satellite networks have become a cornerstone of modern military operations, but their increasing reliance on commercial entities introduces new vulnerabilities. As adversaries develop more sophisticated cyber and electronic warfare capabilities, the resilience of these satellite systems must be prioritized. Future conflicts will be shaped not just by who controls space-based infrastructure, but who can defend it against emerging threats.

📎 [Read the full report here]

Tab 6 – Space ISAC Forum Post

Plain Text – Tab 6

Shows a webpage of spaceisac.org and navigates user to collaborative groups page. Header Image reads: Space ISAC, collaborating to protect our space assets, information sharing and analysis center. Dated September 8th, 2025.

Spaced ISAC Forums: LEO Owner Operators Affinity Group

Conversation on Forum Reads:
Zainab (ESA): NORAD is reporting that none of the satellites are altering their trajectories, and they're not seeing any new assets that weren't already tracked from launch last week. Everyone is where they're supposed to be.

DidiF (S3): Is anyone other than LEO seeing these outages? Any geostationary ones?

DA (USSTRATCOM SA Red Team): I can check, but AFAIK nobody else is seeing this as regularly as we are, if they're seeing it at all.

FreeBird (Seradata): We're in the Analyst Working Group too, but nobody there has any data that we haven't already supplied. UC Colorado Springs is helping to analyze the signal jamming now that the geomagnetic storm is over. We're pretty sure it's not coming from any ground tracking stations, otherwise it would be hitting every satellite that hits a given station. Looks like it's only L band, not Ka or Ku. Which doesn't help those of you with older hardware, sorry.

DA (USSTRATCOM SA Red Team): Unless there's a tracking station that's deliberately targeting specific satellites.

Zainab (ESA): Not everything is an attack, Danny. You red team folks are all so paranoid.

DA (USSTRATCOM SA Red Team): If I were doing this, I'd do my best to make it NOT look like an attack, I'm just saying.

DidiF (S3): Latest launches were from O Corp. They're not members here, right? If not, they ought to be.

FreeBird (Seradata): Yeah, like that's going to happen LOL

Zainab (ESA): Unfortunately if we hear anything in the AWG, and it's classified, we won't be able to share it over here, as per usual. DM me if there's something you really need to know and I'll see if I can pass on something that helps.

DidiF (S3): Thanks Zainab, do you like chocolate? (;

Tab 7- Internal Emails

From: Dr. Isabelle Laurent <ilaurent@esa.int>
Sent: Tuesday, September 9, 2025 9:38 AM
To: James Carter <jcarter@ocorp.com>
CC: ESA Spectrum Management Team <spectrum@esa.int>
Subject: Inquiry Regarding L-Band Interference Observed from O Corp Satellites

Dear Mr. Carter,

We are reaching out regarding a recurring issue we have observed in our trajectory analysis concerning ground station communications. Specifically, we have noted that communications tend to be disrupted when our ground stations are in the line of sight of certain satellites in the O Corp constellation. Our data suggests that these satellites are jamming all frequencies in the L band (1-2 GHz), resulting in outages lasting approximately 20 minutes per affected station as the satellites pass overhead.

This interference has been observed along a consistent geographical path that matches the orbital trajectory of O Corp's satellites. Given the potential impact on critical space-based operations, we would appreciate any insights you can provide regarding whether this interference may be related to O Corp's satellite transmissions.

Please let us know if we can coordinate further technical discussions to better understand and mitigate this issue. We appreciate your cooperation in ensuring the continued safe and effective operation of satellite communications.

Best regards,

Dr. Isabelle Laurent
European Space Agency (ESA)
Head of Spectrum & Communications Division

From: James Carter <jcarter@ocorp.com>
Sent: Tuesday, September 9, 2025 12:14 PM
To: Dr. Isabelle Laurent <ilaurent@esa.int>, ESA Spectrum Management Team<spectrum@esa.int>
CC: O Corp Legal & Regulatory Compliance <legal@ocorp.com>
Subject: Re: Inquiry Regarding L-Band Interference Observed from O Corp Satellites

Dear Dr. Laurent,

Thank you for reaching out regarding your concerns about ground station communications. We acknowledge your observations and want to assure you that any potential issues with O Corp's satellites are being reviewed internally. However, please note that we are unable to share proprietary operational data or technical details with ESA or any external parties.

Should there be any regulatory concerns, we recommend addressing them through the appropriate national and international spectrum management bodies.

Best regards,

James Carter
Director of Operations
O Corporation

O CORPORATION
Connect the World

From: Dr. Isabelle Laurent <ilaurent@esa.int>
Sent: Tuesday, September 9, 2025 1:28 PM
To: James Carter <jcarter@ocorp.com>
CC: ESA Regulatory Affairs <regulatory@esa.int>, ITU Spectrum Coordination <spectrum@itu.int>,O Corp Legal & Regulatory Compliance <legal@ocorp.com>
Subject: Re: Inquiry Regarding L-Band Interference Observed from O Corp Satellites

Dear Mr. Carter,

Thank you for your response. While we understand that O Corp cannot disclose proprietary data; the issue at hand directly affects the integrity of ESA's ground station operations. Given that the interference is persistent and aligns with your satellite trajectories, we urge O Corp to clarify whether any intentional or unintentional emissions in the L band could be responsible.

As you are aware, sustained interference in this frequency range may raise compliance concerns under international spectrum coordination agreements. ESA may need to escalate this matter to relevant regulatory bodies, including the International Telecommunication Union (ITU) and national authorities, should the disruptions continue.

We would appreciate the opportunity to discuss potential mitigations to ensure uninterrupted operations for all parties. Please let us know if a technical dialogue can be arranged.

Best regards,

Dr. Isabelle Laurent
European Space Agency (ESA)
Head of Spectrum & Communications Division