G & A Engineering

AEROSPACE CYBERSECURITY

CHI SONO

I am Giorgia, Electronic Engineer and Astronautical Engineer.
CEO of G & A Engineering, CTO of Ferrari Farm Società Agricola.
Vice President and Secretary of the Space Exploration Commission at the Order of Engineers of the Province of Rome, Member of the Board of Directors of Women4Cyber Italia, Vice President of Anima Reatina.
The passion for agriculture has always accompanied me, passed down from my family of humble peasant origins, as well as the passion for technology that is constantly evolving, because dynamism is the best weapon to know and know yourself better.

Working from over 45 years in Space, Defence, Automotive & challenging Professional Electronics sectors.

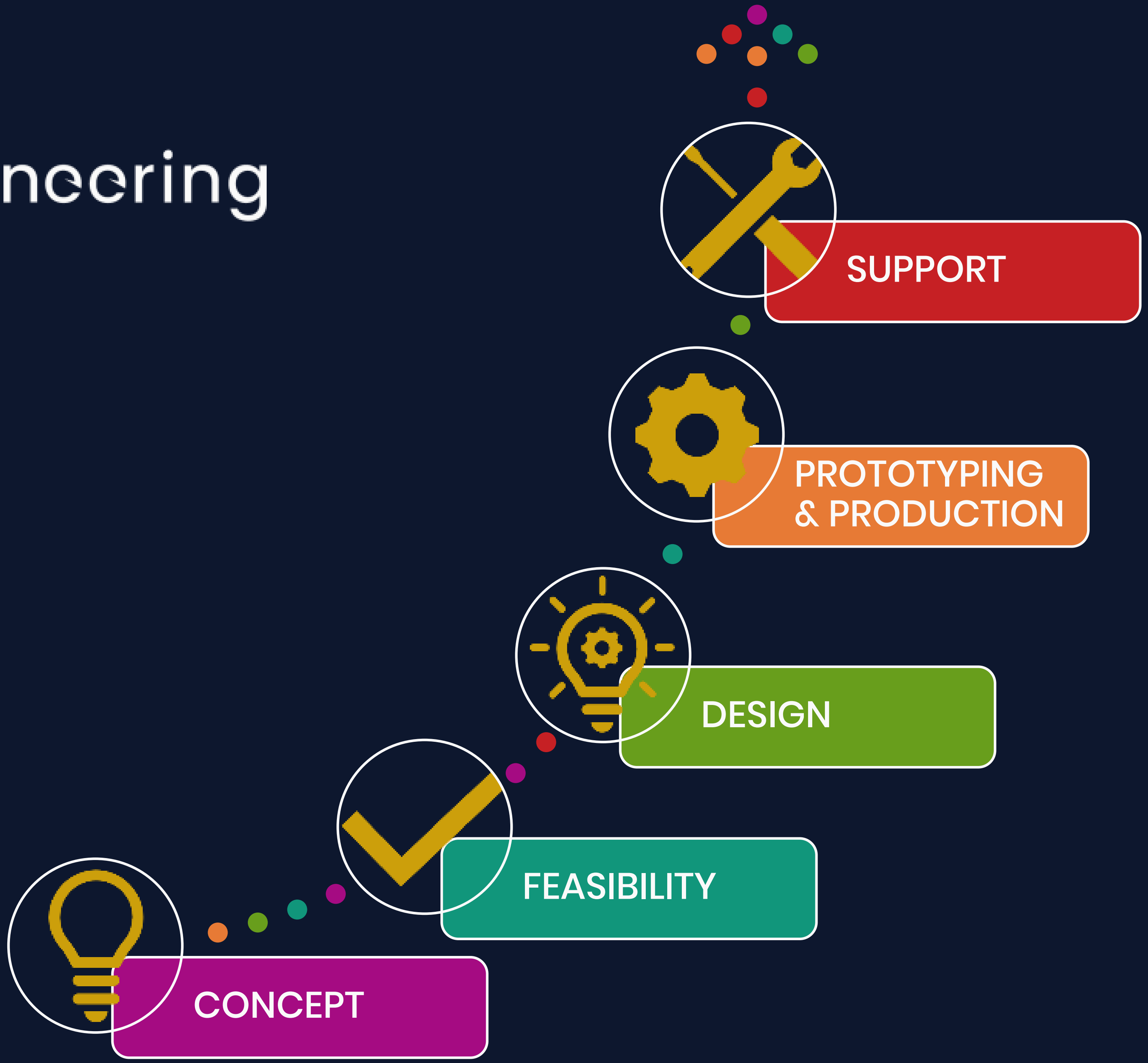
Main Business:

Design and development of sophisticated and complex systems composed by the combination a mix of technologies.

STS-134

DaMa Mission

G&A Engineering



CONCEPT

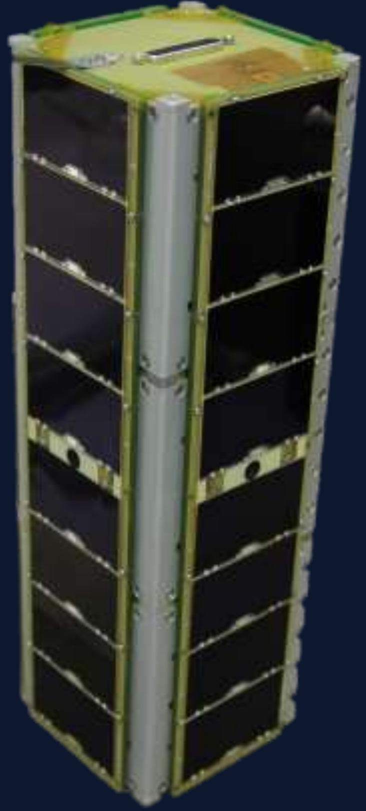
FEASIBILITY

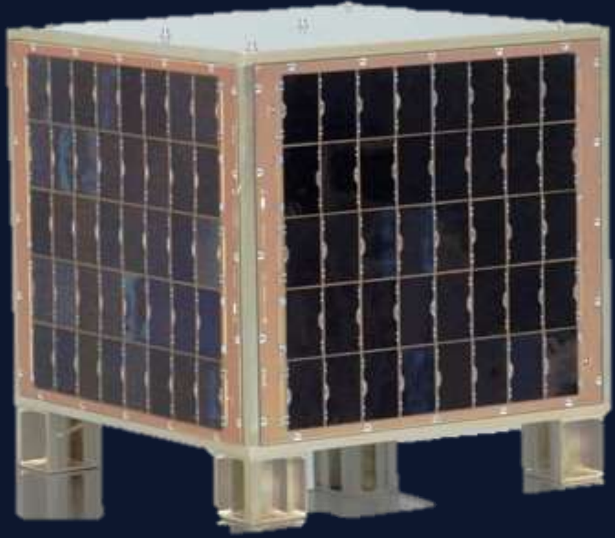
DESIGN

PROTOTYPING & PRODUCTION

SUPPORT

G&A Engineering





SPACE

Space activities are crucial to the functioning of modern societies, from economic activities to those in the field of security and defense.

Given the critical nature of space infrastructure, it risks being the target of a wide range of attacks, including cyber.

The cyber threat to space systems is constantly evolving, also characterized by a potential convergence with electronic warfare tools.

SPACE

Space activities have concrete effects on the functioning of society as a whole.

The case of global satellite navigation services such as Galileo is particularly significant, as many activities depend on them, from finance, to mobility, to energy but also response and management to disasters and emergencies.

The military sector is also strongly connected and dependent on space assets, both in the case of positioning, navigation and synchronization services (Position Navigation and Timing, PNT) and of Earth observation and satellite communication.

SPACE

The space and cyber domains are strictly interdependent: on the one hand, the latter is enabled by assets in orbit; on the other, space systems depend on the exchange of data that occurs in the cyberspace spectrum.

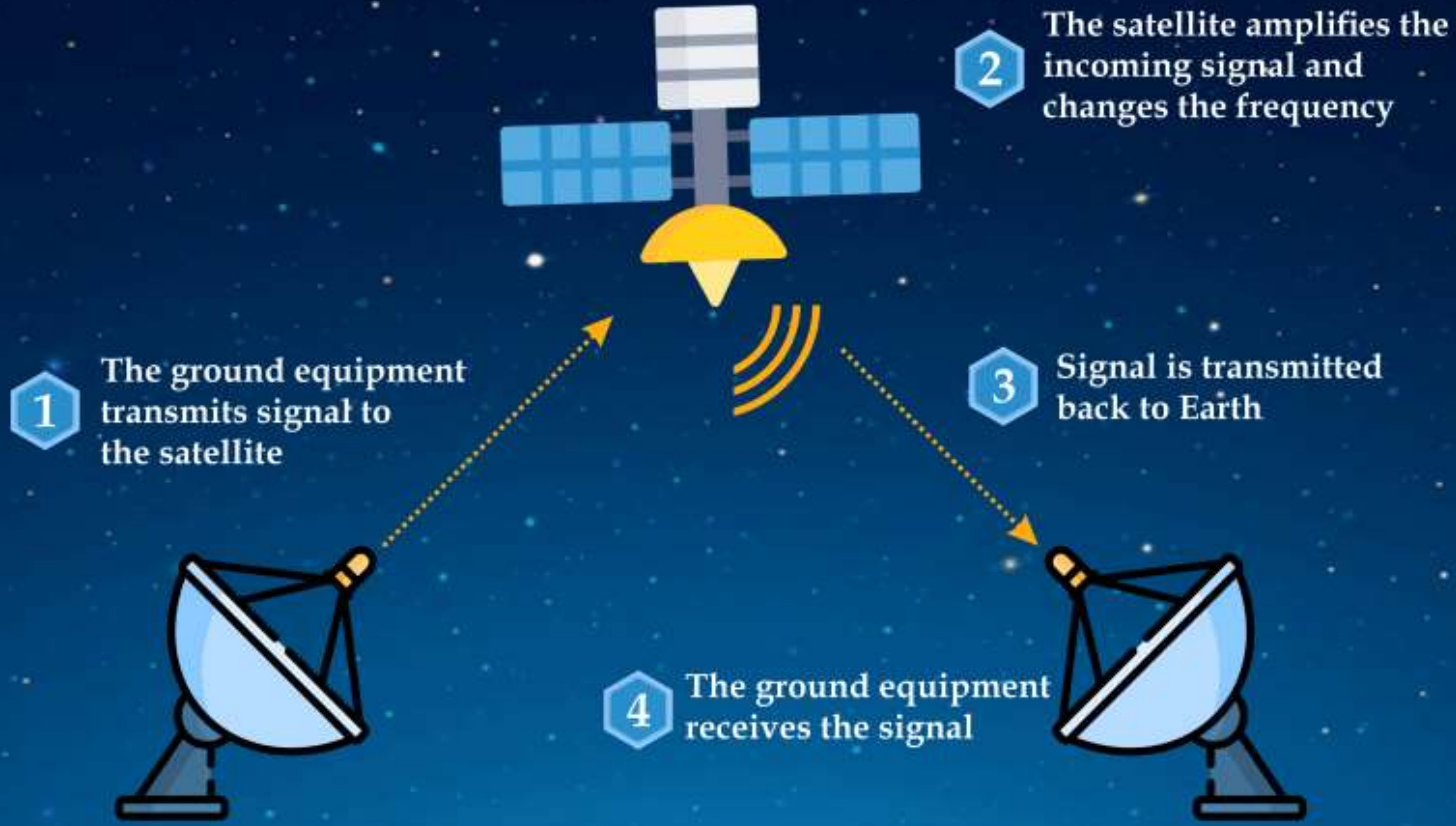
In addition to being interdependent with each other, the space and cyber domains are interdependent with the traditional terrestrial, air and naval domains, in the perspective of multi-domain military operations and technological development towards new generations of weapon systems necessarily integrated with the space and cyber dimensions.

SPACE COMPONENTS

Talking about security in the Space Segment, we have to focus on 2 fundamental components of the segment:

1. The Space-Terrestrial or Ground Stations
2. The Space-Satellite or the Satellite in orbit.

GEA Property 2024



1 The ground equipment transmits signal to the satellite

2 The satellite amplifies the incoming signal and changes the frequency

3 Signal is transmitted back to Earth

4 The ground equipment receives the signal

SPACE SEGMENT

- Command Intrusion
- Payload Control
- Denial of Service
- Malware

USER SEGMENT

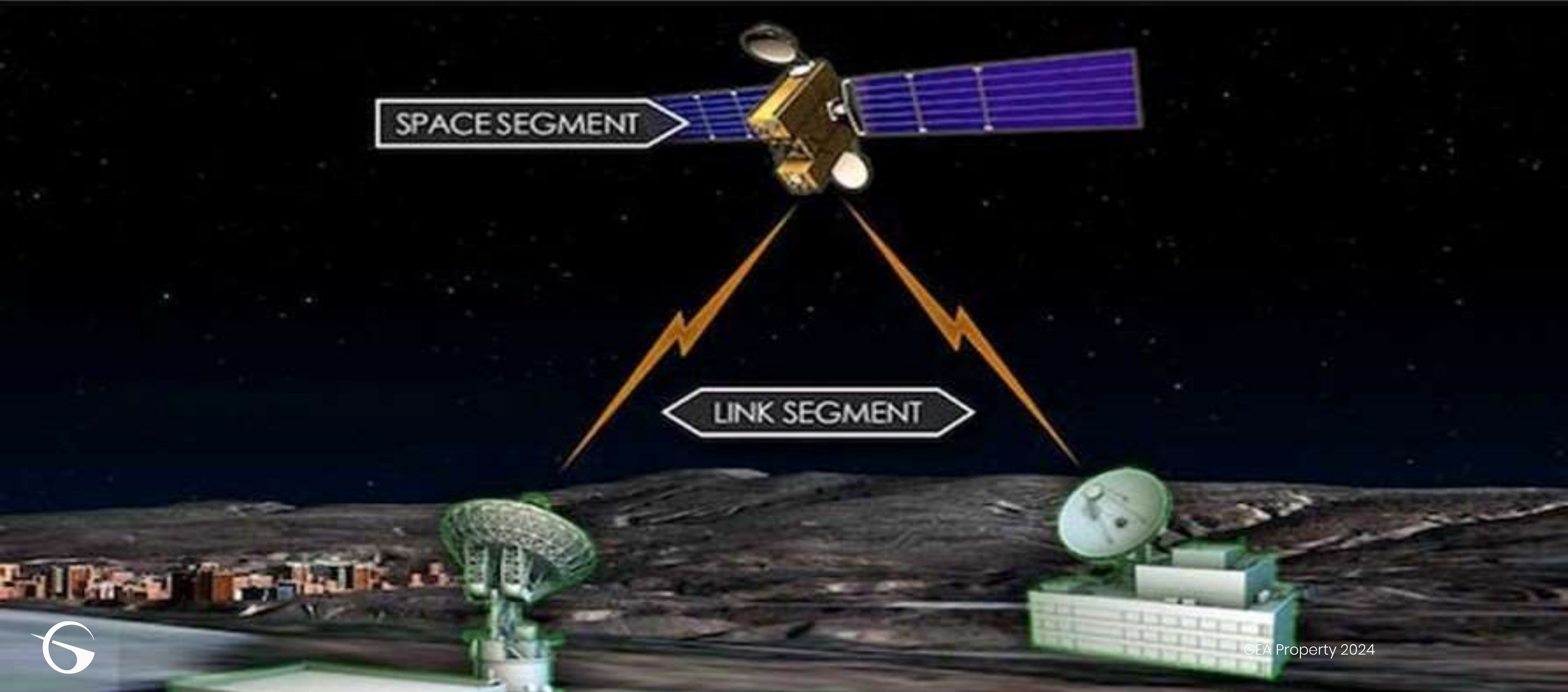
- Spoofing
- Denial of Service
- Malware

LINK SEGMENT

- Command Intrusion
- Spoofing
- Replay

GROUND SEGMENT

- Hacking
- Hijacking
- Malware



SPACE VULNERABILITIES

With the continuous proliferation of small satellites in Low Earth orbit, cybersecurity is something that the community is forced to take seriously.

With the low cost of small satellites controlled by commercial off-the-shelf (COTS) hardware, open-source software (mostly Linux based) and web-based ground station services, the likelihood of vulnerability clearly increases.

SPACE VULNERABILITIES

Vulnerabilities in space assets may present along the whole supply chain, which includes design, development, launch and operation of space objects.

In addition to that, there are 3 important factors in the production and operation of space assets that expand the vulnerability window:

1. Encryption of space assets (satellites) exponentially increases the costs and reduces efficiency of the asset.
2. Vulnerabilities remain unpatched during the long lifespan (satellites lifespan between 5 and 30 years).
3. Several space assets use COTS with low cybersecurity standards.

SPACE VULNERABILITIES

- Attacks on corporate IT networks could be characterized by exploitation of misconfigured or vulnerable technologies to gain unauthorized access to the ground control stations.
- The cloud infrastructure, powers the majority of the computing framework in the ground station. From data storage to data processing, the entire service platform is dependent on cloud infrastructures. Failure of the cloud infrastructure could have catastrophic effects on the ground station including denial of service (DoS) for the satellite data receiver.

SPACE VULNERABILITIES

- Supply chain attacks including loss of software and connected instrumentation and the use of shared components between multiple actors, exposes the system to vulnerabilities that are embedded in the supply chain.
- Previously distributed outdated and unpatched COTS software exposes the system to very dangerous attack surfaces.
- The addition of propulsion systems raises additional concerns because there is the potential for a malicious actor to take control of the spacecraft and use it to target and collide with another spacecraft.

SPACE VULNERABILITIES

When Iridium was created as a satellite constellation to provide GPS services to the Pentagon, cybersecurity was not a concern. Yet things changed drastically, and space cybersecurity became a concerning issue.

NASA has increasingly become a target of a sophisticated form of malicious cyber activity designated as “Advanced Persistent Threats” (APTs). This term is used to refer to State or non-State actors, with both the capacity and intent to persistently and effectively target a specific organization, to steal or modify information from computer systems and networks over a long period without being detected. The NASA 2019 report acknowledged being a regular target of malicious cyber activities.

SPACE VULNERABILITIES

Researchers were able to broadcast a conference using a disused satellite, highlighting the potential risks of a lack of controls.

Hacking a satellite in space for demonstration purposes, to understand what vulnerabilities there are and increase the resistance of systems in orbit in the event of real attacks. This is the idea behind the attack simulation conducted on April 25 2023 by a team of 4 ethical hackers from the aerospace giant Thales, during the largest European exhibition dedicated to cybersecurity in space, the Cysat in Paris.

SPACE VULNERABILITIES

For the first time in the world, an ethical hacking session was successfully attempted on a satellite in orbit.

The target was the European Space Agency (ESA) flying laboratory Ops-Sat, a satellite the size of a shoe.

The hackers of the Red Team Thales identified and exploited the vulnerabilities of the on-board electronics to disrupt the operations of the various devices on board such as the camera, GPS, ACDS control system and radio.

At the end of the demonstration, ESA regained control of the satellite, and the vulnerabilities highlighted were immediately closed, thus increasing the resilience of the satellite to possible cyber attacks.

SPACE DOMAIN

Keeping space systems secure from malicious attacks is essential in today's world where satellites provide vital services from resilient communications to banking, to directing autonomous cars.

Spacecraft in orbit and the systems on ground that fly them can be targeted by malicious attacks.

Cybercriminals can destroy or damage strategic services and crucial data or leverage compromised space assets to support hybrid attacks against others.

SPACE DOMAIN

Rogue states could use a compromised ground station or their own facilities to interfere with a satellite's command & control communications, intercept valuable information, or use lasers to blind a satellite from the ground.

Terrorist groups could use satellite jammers to create electronic interference with a satellite's signal, send spoof signals, place malware in satellites themselves or eavesdrop on sensitive information relayed via satellites.

Even small but well-organised groups of cybercriminals could use experimental strategies to exploit the vulnerabilities of space systems to gain public recognition and visibility.

HACKING THE SPACE

Hacking a ground station could lead to gaining the command and control of a satellite, shut down all communications and permanently damage the space object.

It could also deny, degrade or manipulate the satellite transmission, or even access to information captured by the satellite through its sensors.

The hacker might delete or replace the encryption keys of the space object and establish communications with nefarious purposes.

The malicious cyber activity can also affect the manoeuvring of a satellite, making it collide against another one, decay or lower its orbit until it re-enters the Earth, burns up and ends the mission.

HACKING THE SPACE

The OBC of a satellite can allow reconfiguration and software updates, which increases its vulnerability. These vulnerabilities enable an attacker to target and directly affect the space object in orbit.

The isolation of satellites in orbit and their reliance on wireless communications expose them to specific threats such as signal jamming, spoofing, disguising communications from a suspicious source as those of a known, trusted source and the interception of data.

Additionally, the limitations on processing power and bandwidth in space exacerbate the challenge of implementing routine software updates and patches, leaving systems vulnerable to exploitation.

MALICIOUS SPACE CYBER ACTIVITIES

SPACE CYBER INTERFERENCE

An activity with temporary disruptive effects.

Applied to space systems, interference can cause the temporary unavailability of data or the delay in its transmission.

Even if space interference is not destructive per se, it may also have destructive consequences if, due to the temporary interference, an avoidance manoeuvre is hindered and damage is caused in flight.

It might also cause destruction on Earth if, for instance, a GPS satellite is interfered and delayed information is delivered to a military operation.

MALICIOUS SPACE CYBER ACTIVITIES

SPACE CYBER ATTACKS

Space cyberattacks can be placed in a different level of threats since they produce destructive consequences:

- Full destruction of the satellite
- Destruction of essential elements for the life of the satellite
- Destruction of critical instruments for the mission
- Data destruction

MALICIOUS SPACE CYBER ACTIVITIES

SPACE CYBER ESPIONAGE

This one is neither disruptive nor destructive.

Cyber espionage has been defined as the act or practice of obtaining secrets from individuals, competitors, rivals, groups, governments and enemies also for military, political, or economic advantage using illegal exploitation methods on internet, networks, software and/or computers.

Cyber espionage can be carried out for exploratory purposes, i.e. to conduct preparatory intelligence actions for a potential and future malicious cyber activity that might have either destructive or disruptive effects. In such cases, cyber espionage might be considered the first stage of space interference or of a cyberattack.

SPACE DOMAIN

In an increasingly digital word, security and privacy concerns are becoming a growing priority focus for institutions, consumers and businesses.

Satellite communications' dependence on digital technologies, together with the growing use of commercial off-the-shelf (COTS) components, has led to the extension of the attack surface throughout satellites' lifecycles.

To sustain competitive advantage over the coming decade, satellite communications need to adopt innovative security technologies and state-of-the-art, security-by-design processes.

SPACE DOMAIN

At the same time, satellite communications offer a unique alternative to the transmission of data through the terrestrial internet, where it is increasingly vulnerable to potential malicious attacks.

Used either as a primary communication means or as a back-up to terrestrial networks, satcom can therefore enhance the security of sensitive data transmission and storage or provide back-up connectivity in case of cyberattacks.

This can benefit a wide range of sectors such as transportation, finance, business and government.

SPACE DOMAIN

Space systems are critical infrastructures and thus play an important role in State security and international stability.

Space security, space safety and long-term sustainability of outer space activities cannot be disassociated but require a holistic approach.

Progress in cybersecurity measures in outer space is not just a technical necessity but a global imperative, to safeguard the future of space exploration and the integrity of critical space infrastructure.

Addressing the evolving landscape of cyber threats demands ongoing vigilance, innovation, and a unified approach among all those involved in spaceflight.

CHALLENGES

Although many space components already implement cybersecurity measures to ensure the availability, confidentiality and integrity of information, the current overall level of cybersecurity of most existing satellite infrastructures is not satisfactory.

Existing international policies, whether related to the space or cyber domains, are not up to the challenges that EU and NATO states will face in the years to come.

CHALLENGES

The cybersecurity of space systems should be considered a priority issue to be addressed urgently, especially if we consider the growing technical and technological capabilities demonstrated by actors (state and non-state) considered hostile and the level of dependence of advanced societies on the services offered by these systems.

This is in addition to the fact that there is a frequent problem of obsolescence of the software present in satellites currently in orbit, created in the analog era, before the affirmation of the security by design approach, and therefore intrinsically vulnerable.

CHALLENGES

Space agencies, the satellite industry, cybersecurity researchers, nongovernmental bodies, and intergovernmental satellite organizations show increasing awareness of the space cybersecurity challenge.

Protecting space activities requires understanding the particular cyber vulnerabilities that arise in various space operations.

For example, satellite cybersecurity encompasses the satellite itself, transmissions to and from Earth, and ground stations.

Improving space cybersecurity requires extending good cybersecurity practices into the commercial space sector and addressing problems specific to space activities.

CHALLENGES

Actions at the national, industry, and international levels can harness growing awareness about space cybersecurity and strengthen policy and industry practices as the convergence of space and cyberspace accelerates.

Outer space might not be the “final frontier for cybersecurity,” but achieving cybersecurity beyond Earth is one of the many responsibilities the new era of space activities creates for governments and societies.

SPACE ATTACK

Recent cyber incidents, such as the 2022 attack on the Viasat KA-SAT network, have served as stark reminders of the growing vulnerability of our satellite infrastructure.

This disruptive assault, which interrupted Internet access for thousands across Europe, highlighted the strategic significance of satellites as critical targets for cyberadversaries.

These events are not isolated incidents, they mark an escalating trend as sophisticated cyberactors increasingly recognize the potential for devastating disruption through satellite-based attacks.

The incident prompted an international call from the European Parliament for stronger cybersecurity measures in space technology, emphasizing the need for enhanced cyber-resilience

SPACE ATTACK

The vulnerability of satellite systems to cyberattacks is no longer theoretical.

This incident, along with others monitored by organizations such as ENISA - European Union Agency for Cybersecurity and the CyberPeace Institute, highlight the growing threat posed by cyberadversaries targeting satellite infrastructure.

A study by ENISA found that the number of such attacks has increased by 300% in the past 5 years, with a particular focus on disrupting critical satellite-based communication systems.

SPACE CYBERSECURITY NEEDS

We need immediate, fortified satellite cybersecurity, not as a distant aspiration but as an urgent imperative right now.

This is not a call for vague future planning but a demand for decisive action now to avert an all-too-likely scenario where critical services are incapacitated with far-reaching and devastating consequences.

Cybersecurity experts, including those at NASA and the European Space Agency, stress the importance of developing robust encryption and secure communication protocols specifically tailored for satellites.

These measures are essential to protect sensitive data and prevent unauthorized access to critical satellite systems.

SPACE CYBERSECURITY NEEDS

By taking decisive action to fortify our satellite cybersecurity, we ensure that space remains not just a frontier of exploration but also a domain of security and reliability.

Protecting our celestial sentinels is essential to safeguard the very fabric of our interconnected world and thereby ensure the continued advancement of human progress in the digital age.

Today's efforts to secure our satellites will protect our global infrastructure for future generations.

THERE'S NO SAFETY ON EARTH WITHOUT SAFETY IN SPACE

GRAZIE

G&A Engineering

Località Miole snc – 67063 Oricola (AQ)
Via Colle Cerqueto 1 – 02025 Petrella Salto (RI)
info@gaengineering.com
http://www.gaengineering.com
gaengineeringsrl@pec.it

C.F. & P.IVA 01386350662
Capital Stock Euro 91.800,00 i.v.
Registro Imprese Gran Sasso d’Italia
# REA AQ-85325