CYBERSECURITY FOR THE SPACE ECONOMY

The IoT Connection
c21-virtual
The 5th Epoch Series - Hyperconverged TMT Networks: Space + Terrestrial - 24.v2
October 24th, 2024

Space Economy Scenario

The Space Sector in complementarity-alternative to the Terrestrial one, is in great expansion dual-use Civ/Mil thanks to the constant increase in reliability, capacity, performance, components-systems miniaturisation, global coverage of LEO MEO constellations, decreasing cost of technologies and services

SatCom (GEO-LEO), SatEO (LEO), SatNav (GEO-MEO), benefit from the experience gained on Terrestrial for Software-Defined, Virtualisation, Cloudization, Edge, Hyperscaling, AI/ML, Digital Twin, As-a-Service, 5G Slicing

Global development trends currently focused on Multi-Orbit, Multi-Band, In-Flight Flexible Payloads, RF/IF over IP, RF MW to Laser for ISL, 5G NTN (Sat D2D)

Space Economy Market

Estimates and extrapolations from analysts' data differing from each other

World over **400 BUSD**

SatCom 85,66 BUSD 2023

GEO - LEO / CAGR 9,4 %,

forecast period 2022-2032

Includes **SatIoT 1 BUSD** / CAGR 20 %

SatEO 8,8 BUSD 2023

LEO / CAGR 6,92 %,

forecast period 2024-2032

Includes weather satellites MEO

SatNav 216,95 BUSD 2023

GEO - MEO / CAGR 9,5 %,

forecast period 2024-2030

GNSS Core systems GPS (USA), GLONASS (RUS), Beidou (CHN), Galileo (EU)

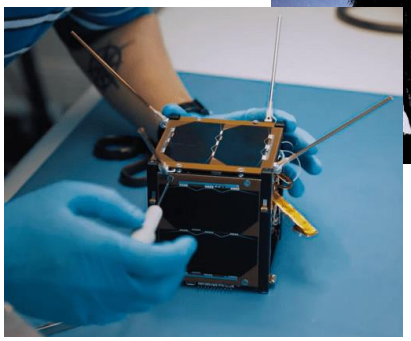
Space Access Launchers **100 BUSD**

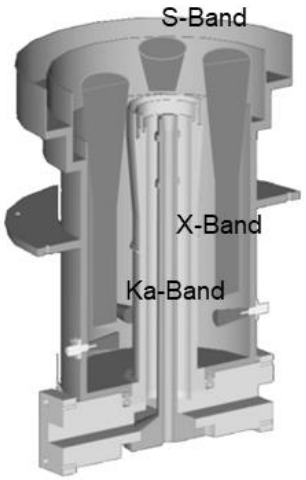
There are currently more than 10,019 active satellites, two-thirds of which belong to the SpaceX constellation.
Most of the active satellites are LEO (9,254)

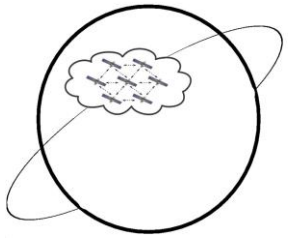
The present greatest activity in space is not from putting satellites into orbit, orbital shifts, payload reconfigurations, etc., but from spy satellites spying on other spy satellites (!)

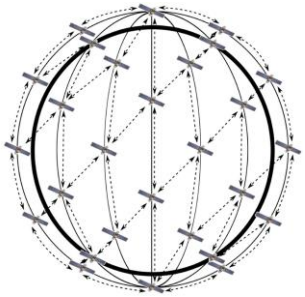
Examples of evolutionary impact in Space/Ground Segment

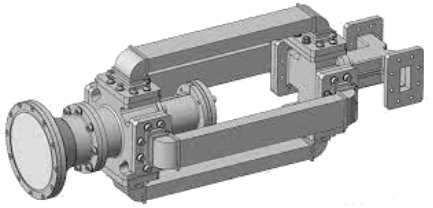
- **Micro/Nano/Pico Satellite Production**
- **Multi-Orbit GEO, MEO, LEO**
- **Networks architectures evolutions of LEO Constellations**
  Space-Time dynamic routing, Collaborative-Autonomous formation flying (Rendezvous & Docking, Swarms, Formation Flying such as Trailing, Cluster, Leader-follower,..)
- **In-Flight Flexible Payload for Missions reconfiguration-updating**
  Electronically Splittable, Shapeable, Steerable
- **Capex Opex reduction and Services expansion thanks to technological evolution, miniaturization, performance, reliability, convergence, interoperability**
  AI/ML, RF Digitization, SD Software-Defined (i.e. radio, modem), Cloudization, Virtualization, Edge, GSaaS,..
- **Multi-Band Multi-Orbit Ground Segment Antennas for SatEO and SatCom (i.e. S, X, K/Ka - Ka/Q/V Bands)**
  Frequency / Band expansion for increased Com throughput (HTS / VHTS), or Earth Observation image data via complex MW circuit techniques for the antenna feeder and autotracking, with Gbps receivers/demodulators







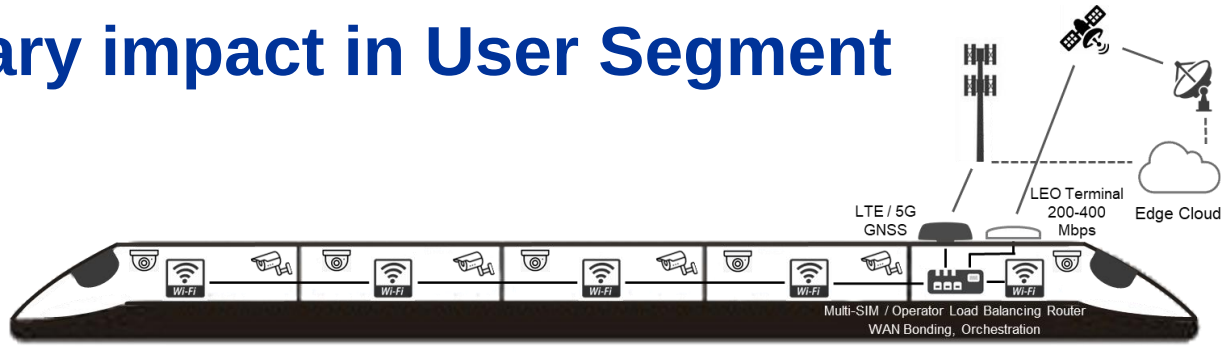




Examples of evolutionary impact in User Segment

B2B/C SatCom

- Internet via Satellite using ESPAA Electronically Steered Phased Array Antennas Terminals, Fixed/On-The-Move over LEO, download of 200 - 400 Mbps



PIS Passengers Information System - IoT - Video Surveillance - Driver Information - Infotainment / Audio Video distribution - Ticketing - Payment System - Train Diagnostics - Emergency Comm

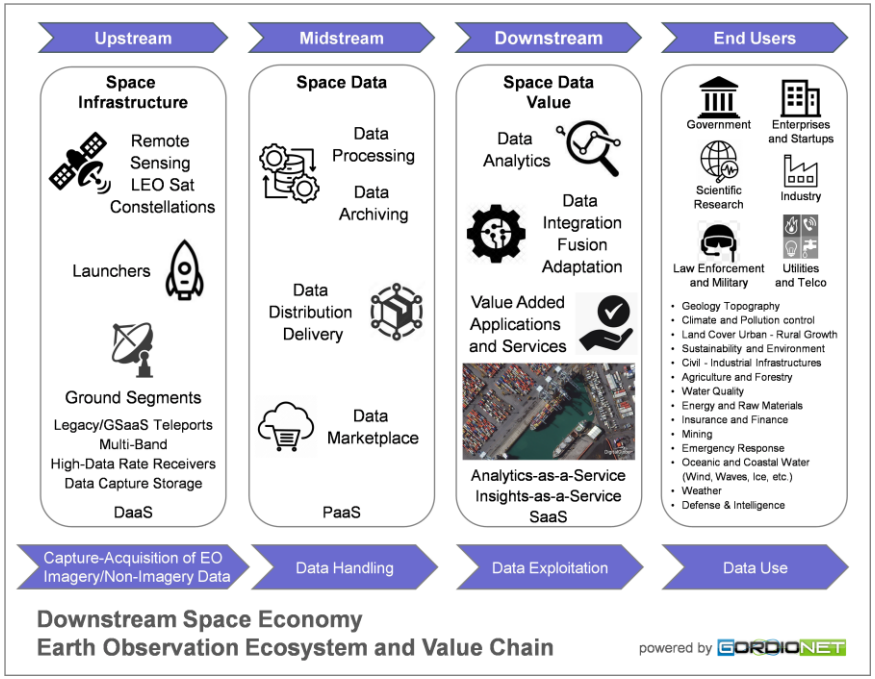


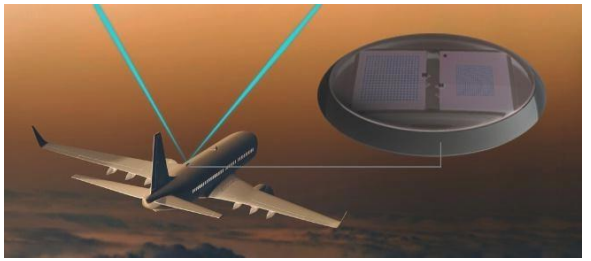


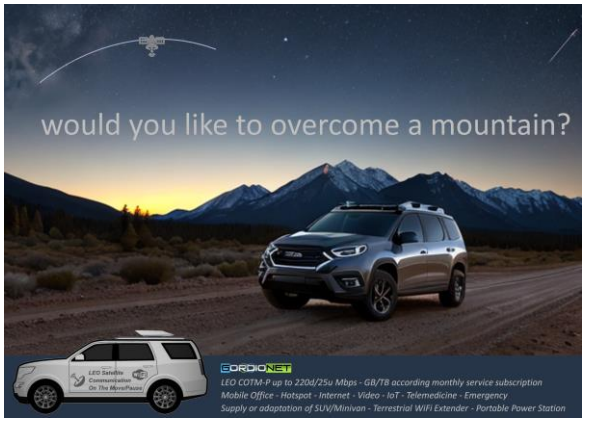
LEO Terminals Business/Enterprise versions

B2B SatEO

- Quality, accessibility, affordability of satellite data
- Continuous evolution of Passive/Active Payload Remote Sensing, with spectral-spatial-temporal-radiometric resolutions increasingly higher
- Increasing capacity of Data Capture-Acquisition, Cloudization, VAS, Analytics/Insight/SW as a Service (Downstream Space Economy)

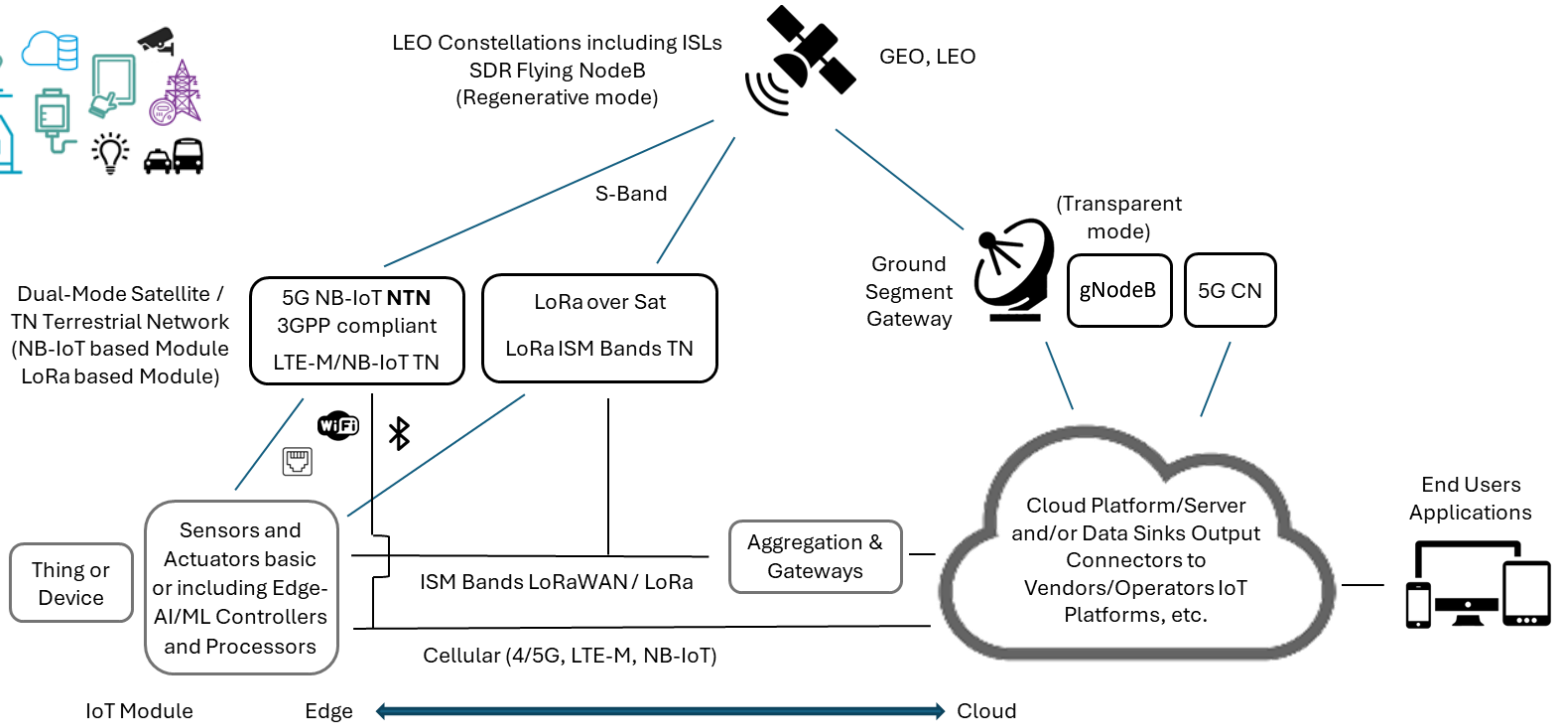






SatIoT - Hybrid Sat/Ter IoT

Agriculture
Maritime
Oil & Gas
Mining
Energy and Utilities
Construction
Military and Defense



According IoT Analytics, IoT Cybersecurity focused since time on the six principles across the stack

Secure Device (HW / SW)
1) Device Intelligence
2) Edge Processing

Secure Communications
3) Device Initiated Connections
4) Messaging Control

Secure Lifecycle Management
6) Remote Control and Updates of Devices

Secure Cloud
5) Identification, Authentication, Encryption

Cybersecurity

The Cybersecurity is no longer considered a technological cost but a business investment, due to serious incidents with economic - financial - competitive - operational - reputational losses

The damages suffered reached a worldwide cost of 8 TUSD, the Cybersec market has surpassed 200 BUSD

Continuously expanding attack surface across Networks, Cloud, Edge, Data Centers, Public/Private Offices, Fixed and Mobile Endpoints, IoT

Third-Party integration and mobility outside the corporate protection perimeter (roaming users - remote/smart working), have greatly extended the area of exposure for data breach, privacy and Malware threats such as Viruses, Worms, Trojans, Bots, Ransomware, Backdoors, Spyware, Adware

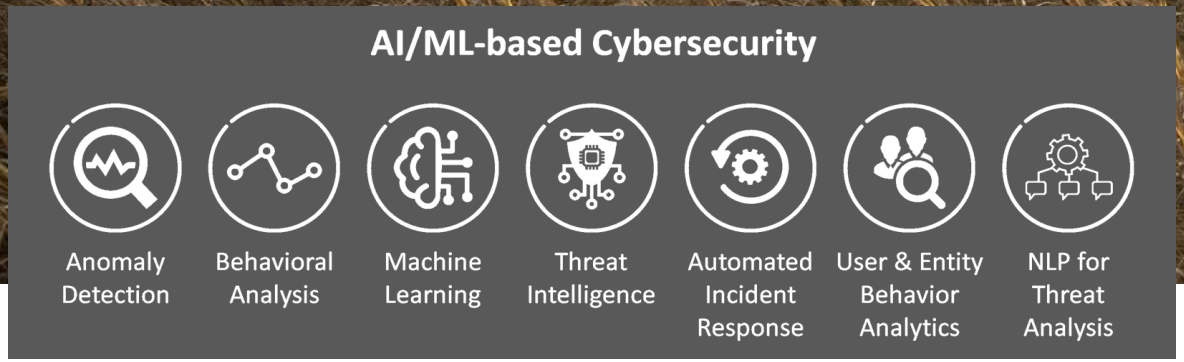
Cyberspace security issues are becoming (are) serious

NextGen Cybersecurity

- Traditional defense measures (Firewalls, IDPS Intrusion Detection/Prevention Systems, RASP Runtime Application Self Protection, Antivirus, AppSec, etc.), are in a situation of passive vulnerability and are no longer sufficient to counter new types of attacks with an increasingly high degree of coordination and intelligence
- Need for defense strategies-tactics of Dynamic Multilayer Cybersecurity for Network-Web/Cloud-Endpoint, with Prediction-Prevention-Detection-Response instead of Mitigation, allowing automatic updates and reconfigurations on flexible Zero-Trust models for Zero-Day vulnerabilities
- Profiling of strategies and technologies according to sectoral segmentations in terms of organisation, processes, production, Supply Chain, vulnerability surface.....

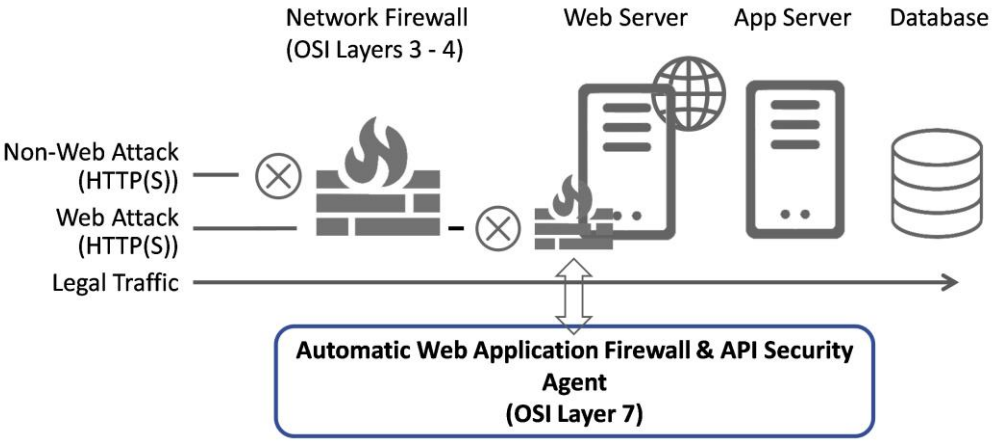
Rule number one: AI/ML-based Cybersecurity

- **AI-based Cybersecurity with ML Machine Learning capabilities is the most powerful tool currently available, although human interaction is essential and irreplaceable in the security field**
- **ML uses existing behavioral models to generate decision-making processes based on previous data and conclusions, and is currently the most relevant Cybersecurity discipline**
- **The new generation of Cybersecurity based on AI/ML - NLP, contemplates dynamic automatic self-learning techniques on behavioral analyses, traffic, databases, without reference to signatures, IP addresses, DNS, etc. (from Signature-based detection to Rule/Scoring-based anomaly detection, including Contextual ML to optimize the Balanced Accuracy i.e. false negative/positive)**

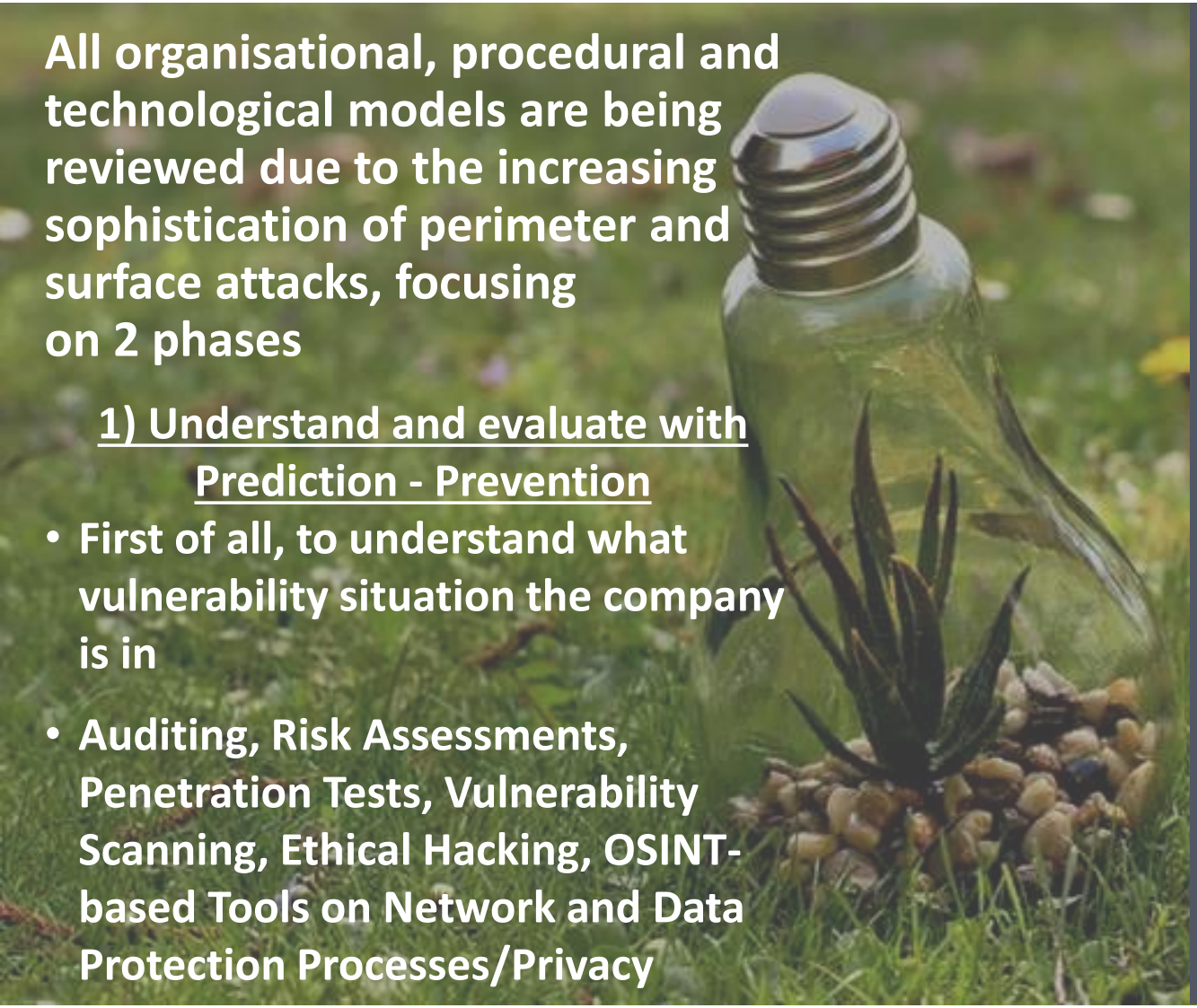


Rule number one (bis): Next Generation Firewall for Network and Web/Cloud Security - API Protection

- WAF Web Application Firewalls are key elements of the infrastructure Cybersecurity for any Web Application or Service, protecting against malicious HTTP traffic and attacks such as SQLi SQL Injection, XSS Cross-Site Scripting, CSRF Cross-Site Request Forgery (i.e. Log4j, Spring4Shell, Text4Shell,..)
- WAFs operate with configurations, patches and rules that involve continuous maintenance of updates for new threats and attack techniques
- Conventional WAFs do not protect, mitigate or block Zero-Day vulnerability attacks, as they should be continuously configured to detect and block dangerous traffic, and can be bypassed by manipulating the string and character payload
- WebApp/Services and APIs are replacing traditional applications with an urgent need to integrate advanced WAF to strengthen security strategies (iWAF, NGWAF)



Cybersecurity Prediction - Prevention - Detection - Response



All organisational, procedural and technological models are being reviewed due to the increasing sophistication of perimeter and surface attacks, focusing on 2 phases

1) Understand and evaluate with Prediction - Prevention

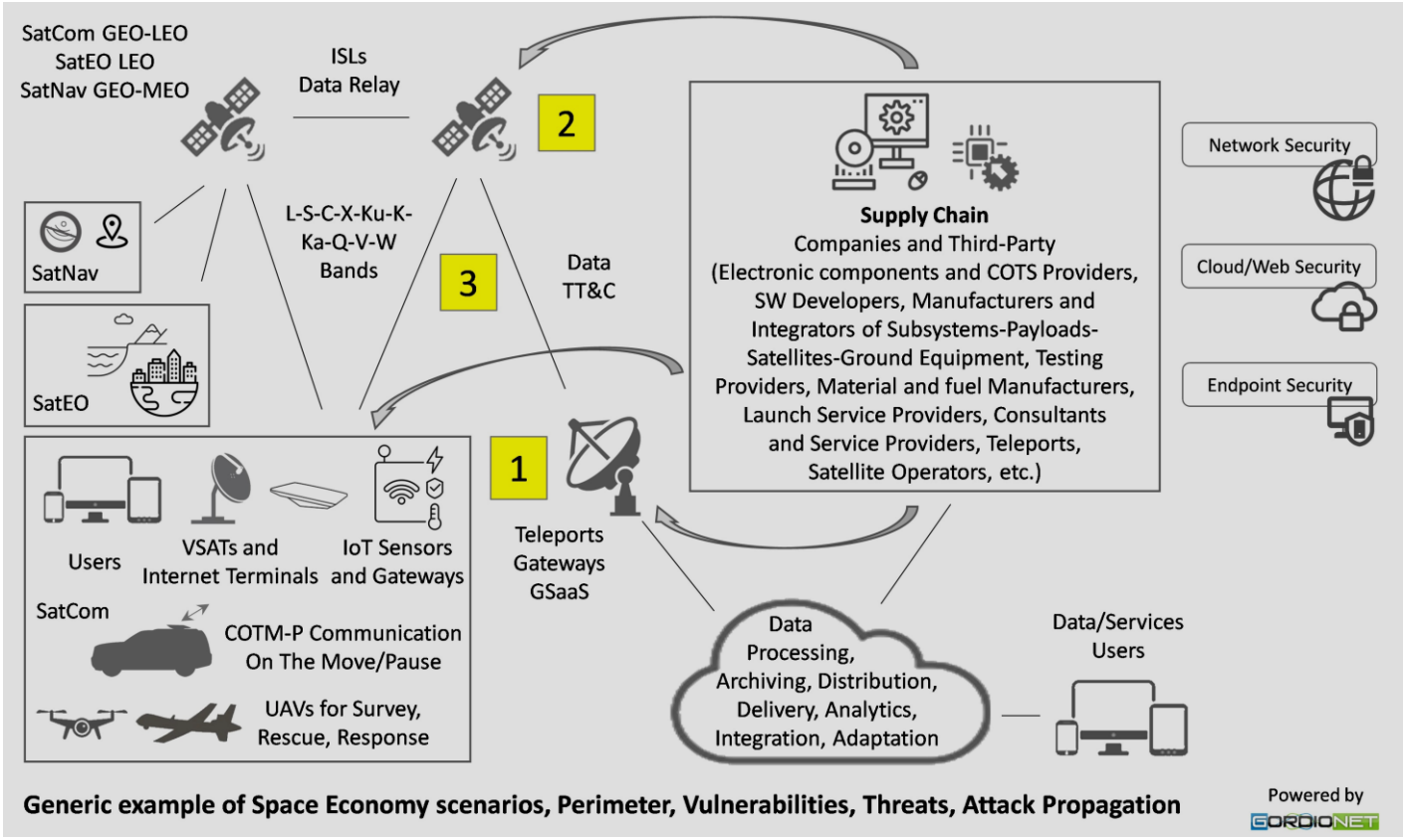
- First of all, to understand what vulnerability situation the company is in
- Auditing, Risk Assessments, Penetration Tests, Vulnerability Scanning, Ethical Hacking, OSINT-based Tools on Network and Data Protection Processes/Privacy

2) Acting with Detection - Response

- From the results of Prediction - Prevention, implement-replace-upgrade the Cybersecurity Detection - Response of Network-Cloud/Web-Endpoint, avoiding expensive HW-SW/OnPrem-Cloud Systems, which are useless if not evolved and not profiled on the exposure of the own vulnerabilities
- No Cybersec brand can guarantee 100 % protection only achievable with Dynamic Multilayer solution bouquets

OSINT

Space Economy, examples of vulnerable areas



EXAMPLES OF RISKS-THREATS WITH CYBERSECURITY NEEDS

1 CNE Computer Network Exploitation - DoS by Network/Cloud Infrastructure failure - Data Corruption/Modification - Supply Chain Attack - Malware Injection in Terminals, Gateways, Sensors - Social Engineering - HW Backdoor

2 DoS (SDR Software-Defined Radio and DSP SW corruption with possible buffer overflow risks) - HW Backdoor - Malware Injection - Privilege Escalation - Hijacking - Sensors Manipulation

RF/Optical and Physical-Kinetic vulnerabilities

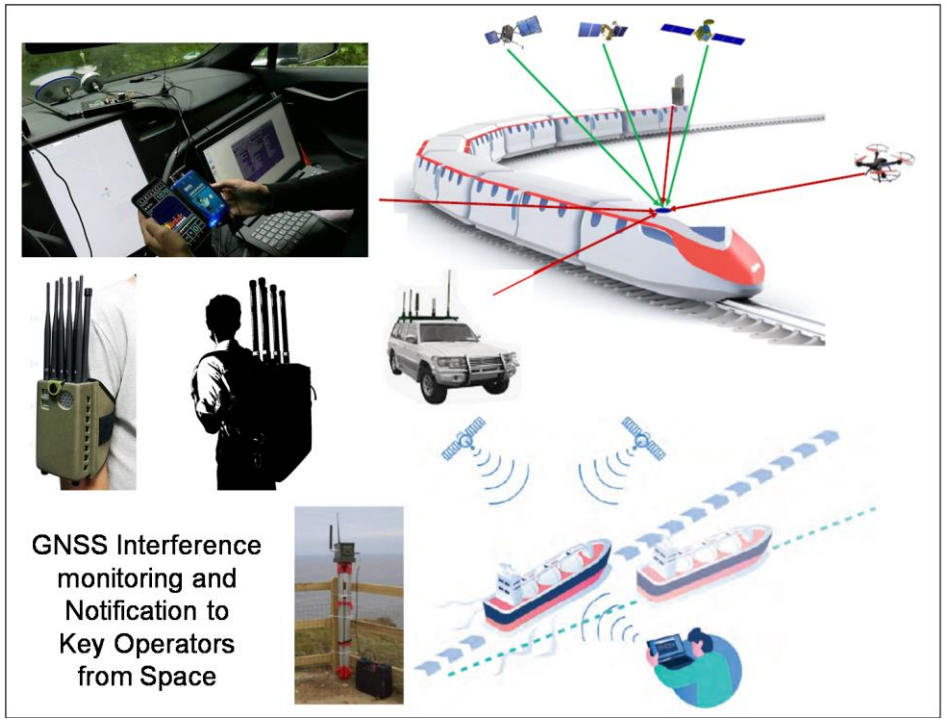
Cyber attack refers to unauthorised non-kinetic or non-physical attacks involving ICT infrastructures and/or devices. RF/Optical and Physical-Kinetic vulnerabilities in any case involve Cybersecurity impacting on Business Continuity - Data Recovery

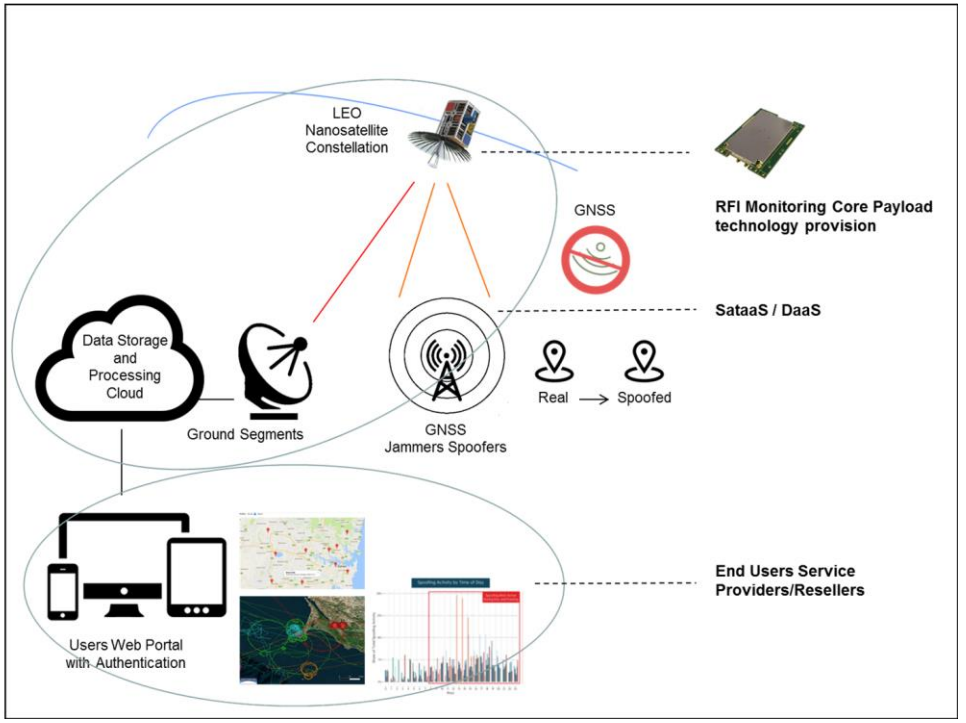
RF/Optical/Comm

3 Jamming (SatCom, SatEO, SatNav) from Signal/Command Injection - Eavesdropping - Satellite Hijacking – Spoofing (SatNav GNSS) - Metadata Analysis - Replay Attacks

Physical and Kinetic Vulnerabilities

Physical Attack of Ground/Space Segments, Orbital Impact, Space Debris on Space Segment (Large Constellations i.e. SpaceX)





Ref: https://navisp.esa.int/project/details/164/show

Space criticality notes

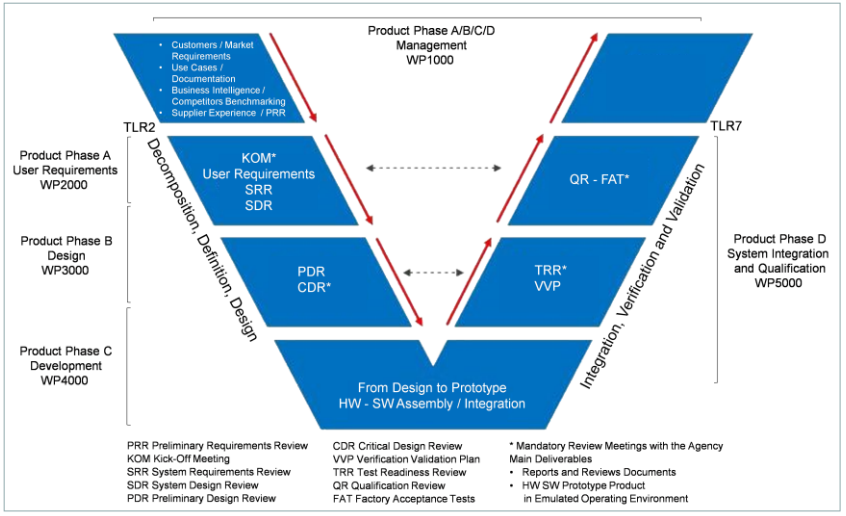
- **Most medium to large satellites are equipped with security measures against attacks, and gaining control of Onboard-Payload systems, exploit SW vulnerabilities, changing their orbit, hacking TT&C channels, requires considerable skills, knowledge, tools-systems**

- **The greatest vulnerabilities are currently concentrated in the Ground-Terrestrial Segment, Supply Chain of the Ground/Space Segment, User Segment**
  Before the invasion of Ukraine, the Russian attack on the ViaSat infrastructure (subsequently partially re-established by Starlink SpaceX) was made on satellite modems-routers

- **Miniaturization and Smartization of Nanosatellites**
  Families of nanosatellites like CubeSats with low construction/launch costs, have no space/budget for Cybersecurity components; Onboard processing in AI-controlled constellations or swarms has increased the vulnerability surface for attacks

- **Existing unmodifiable HW and non-patchable SW**
  Unavoidable bugs in millions of lines of SW code require continuous patches difficult to execute in orbiting satellites, and system updates are generally avoided since a failed update could crash the satellite

- **The Supply Chain is considered particularly critical**
  The attack surface of a long, distributed and heterogeneous Supply Chain has a higher probability of errors and vulnerabilities (e.g. IoT), and plug-and-play integrated COTS (Commercial-Off-The-Shelf) components represent a weakness for strong or consistent security throughout the system



Main Risks-Threats of Segments and Supply Chains

Space Segment

DoS Denial of Service: on Software-Defined Radio (SDR) as digital processing for radio functionality, insufficient control in processing radio frames and sending compromised data packets could cause buffer overflows, creating DoS conditions that block communications

HW Backdoor: vulnerabilities in the satellite's HW components may cause unauthorised access or control over the operational satellite in orbit. HW backdoors may not be immediately evident and may remain undetected over time

Malware: purposefully designed can be introduced into the SW systems of a satellite during assembly, compromising security and functionality once in orbit service with critical detection and removal

Privileges escalation: attempt to increase privileges within the satellite's systems after deployment. Weaknesses in access controls or SW vulnerabilities can be targeted to gain greater control and access over time

Hijacking : unauthorised individuals or entities could attempt to take control of a satellite's systems for their own purposes

Sensors Manipulation: may cause inaccurate data in the orbiting satellite, affecting its functionality and mission objectives

Ground-Terrestrial Segment

Computer Network Exploitation (CNE): attacks on the Network to which the Terrestrial Station is connected similar to those of corporate IT networks, with exploitation of misconfigured or vulnerable technologies, phishing to obtain unauthorised access

Cloud Infrastructure: as Terrestrial Stations are increasingly integrated and dependent on Cloud solutions for storage and processing, they are completely vulnerable to catastrophic DoS effects in the event of a Cloud attack and failure

Data corruption/modification: deliberate or unintentional alteration of data in transit or at rest that may lead to SW failures, HW problems, unauthorised use or attempts to alter data rendering it unusable

Supply Chain Attacks: targeted attacks searching for vulnerabilities and exploits in the supply chain

Malware: malicious SW can infect Terrestrial Station systems compromising security and operations

Social Engineering: manipulation/cloning of individuals to disclose sensitive information or grant unauthorised access to systems

HW Backdoor: exploiting vulnerabilities hidden in the HW of Terrestrial Stations to gain unauthorised control

AI/ML/computer vision Attacks: the use of large language models (LLM) and other advanced AI models has led to a fundamental change in the approach of many activities, and it has been shown that attacks against Machine Learning ML can be implemented effectively

DDoS

The number of attacks against satellite infrastructure has increased by 300 % in the last five years

One method of attack is Distributed Denial of Service (DDoS) from compromised devices, botnets, or multiple attackers or tools

The attack is carried out by sending requests to the target IP address, overloading servers or networks and denying service to normal traffic

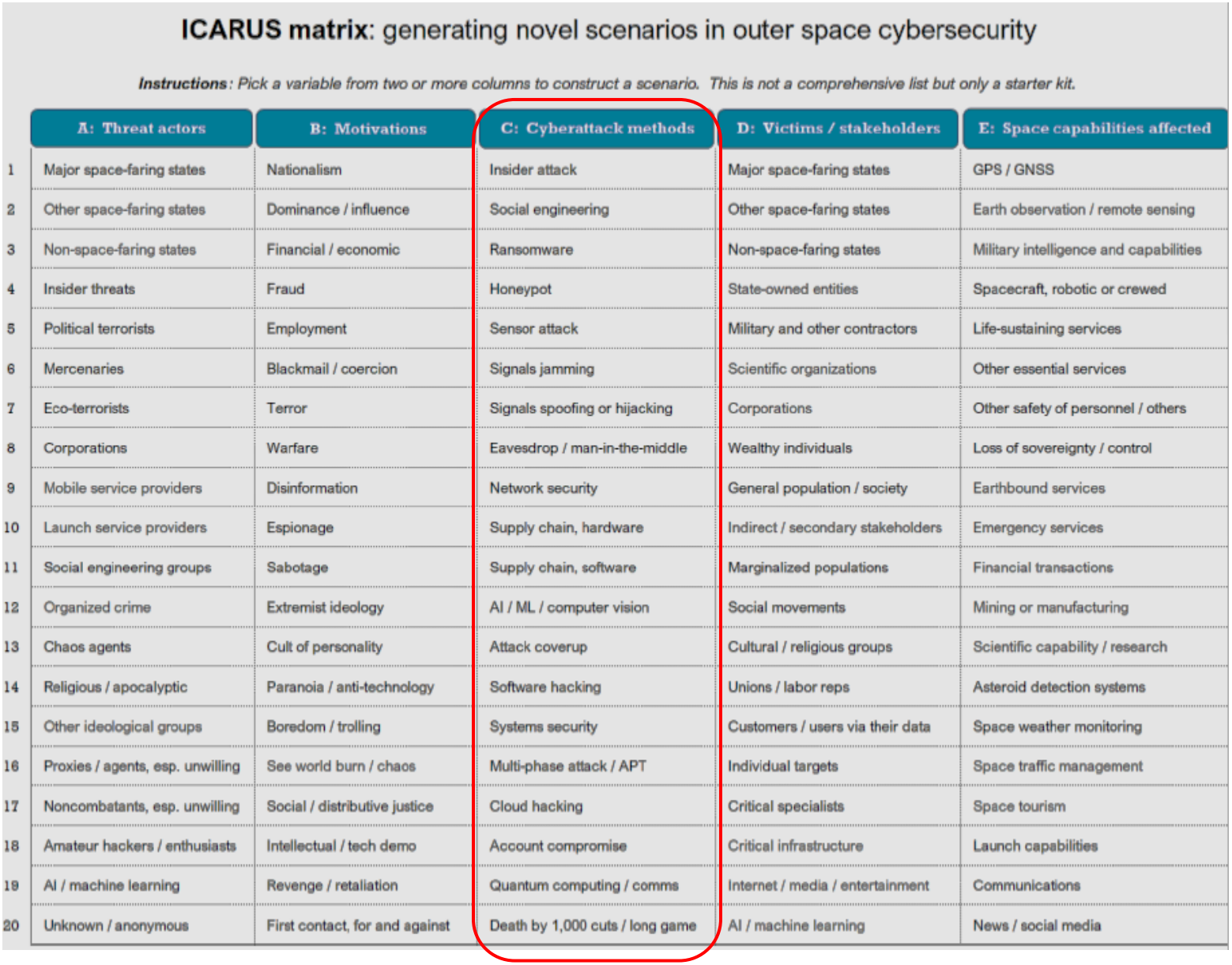
DNS amplification attacks, HTTP flood attacks (get and post) and SYN flood attacks, can cause significant disruptions in data transmission, with loss of control of satellite functions or inability to access critical data

Examples of Supply Chain attack vulnerabilities

Supply Chain attacks can target HW, SW, Apps, devices, systems managed by Third Parties involved in projects, HW-SW production, integration, assembly

- Browser-based attacks
- Software attacks
- Open-source attacks
- JavaScript attacks
- Magecart Formjacking attacks
- HW Backdoor
- Watering hole attacks
- PoC Proof of Concept exploits

ICARUS Matrix*



ICARUS matrix: generating novel scenarios in outer space cybersecurity

***Instructions**: Pick a variable from two or more columns to construct a scenario. This is not a comprehensive list but only a starter kit.*

	A: Threat actors	B: Motivations	C: Cyberattack methods	D: Victims / stakeholders	E: Space capabilities affected
1	Major space-faring states	Nationalism	Insider attack	Major space-faring states	GPS / GNSS
2	Other space-faring states	Dominance / influence	Social engineering	Other space-faring states	Earth observation / remote sensing
3	Non-space-faring states	Financial / economic	Ransomware	Non-space-faring states	Military intelligence and capabilities
4	Insider threats	Fraud	Honeypot	State-owned entities	Spacecraft, robotic or crewed
5	Political terrorists	Employment	Sensor attack	Military and other contractors	Life-sustaining services
6	Mercenaries	Blackmail / coercion	Signals jamming	Scientific organizations	Other essential services
7	Eco-terrorists	Terror	Signals spoofing or hijacking	Corporations	Other safety of personnel / others
8	Corporations	Warfare	Eavesdrop / man-in-the-middle	Wealthy individuals	Loss of sovereignty / control
9	Mobile service providers	Disinformation	Network security	General population / society	Earthbound services
10	Launch service providers	Espionage	Supply chain, hardware	Indirect / secondary stakeholders	Emergency services
11	Social engineering groups	Sabotage	Supply chain, software	Marginalized populations	Financial transactions
12	Organized crime	Extremist ideology	AI / ML / computer vision	Social movements	Mining or manufacturing
13	Chaos agents	Cult of personality	Attack coverup	Cultural / religious groups	Scientific capability / research
14	Religious / apocalyptic	Paranoia / anti-technology	Software hacking	Unions / labor reps	Asteroid detection systems
15	Other ideological groups	Boredom / trolling	Systems security	Customers / users via their data	Space weather monitoring
16	Proxies / agents, esp. unwilling	See world burn / chaos	Multi-phase attack / APT	Individual targets	Space traffic management
17	Noncombatants, esp. unwilling	Social / distributive justice	Cloud hacking	Critical specialists	Space tourism
18	Amateur hackers / enthusiasts	Intellectual / tech demo	Account compromise	Critical infrastructure	Launch capabilities
19	AI / machine learning	Revenge / retaliation	Quantum computing / comms	Internet / media / entertainment	Communications
20	Unknown / anonymous	First contact, for and against	Death by 1,000 cuts / long game	AI / machine learning	News / social media

*Report: “Outer Space Cyberattacks: Generating Novel Scenarios to Avoid Surprise”

Main Reactions

Main Reactions of Prediction - Prevention - Detection - Response

- Vulnerability Scanning
- Encryption, Authentication, Access Control, Revocation
- Secure Protocols
- Network Segmentation
- Browser Isolation
- Routing and Distributed Control
- Redundancy and Backup Systems
- Timely Security Updates
- DoS Prevention-Prediction-Mitigation
- Anomaly Detection and Intrusion Prevention
- Zero-Trust per Zero-Day
- Malware Detection and Blocking
- Detect Shadow IT or CASB Cloud Access Security Broker with Shadow IT detection
- Secure Supply Chain Management and Third-Party Vendor Assessment (may include CSP Content Security Policies o SRI Subresource Integrity to check suspicious content on JavaScript)
- Regular Audits and Testing
- Incident Reporting and Response
- User Education
- Regular Security Training
- DevSecOps, Secure Design Principles and Standards in Spacecraft Design

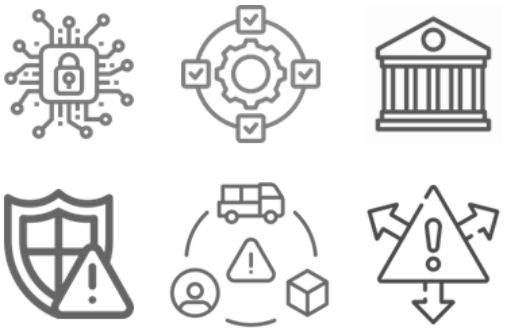
NIS2 Directive

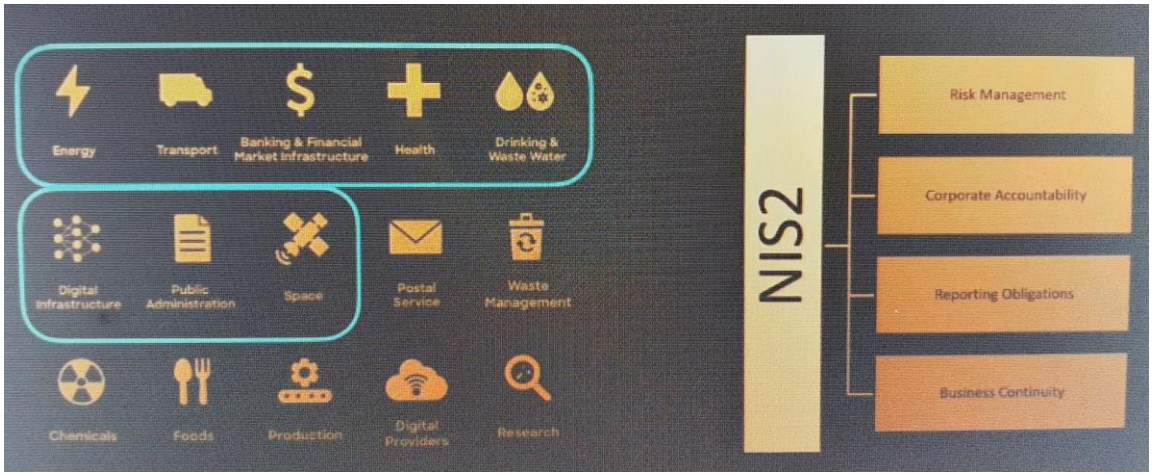
Proliferation of micro-nanosatellites, large constellations, smartization of Supply Chains, quantity and sophistication of cyber attacks, is pointing towards a military-style control philosophy, to prevent anyone from putting a satellite into orbit without the appropriate quality checks with the risk of compromising other satellite networks

National, European and international regulations dominated by the NIS2 Directive monitored by ENISA, which imply compliance with these regulations by large, medium-sized, critical-strategic companies in the Space Sector, non-compliance with which carries heavy administrative or criminal penalties

Management and Awareness, **Reporting to Authorities** (Reporting & Collaboration), **Risk and Incident Management** (Company and Supply Chain Security), **Business Continuity**

Applied to companies with more than 50 employees with a turnover/budget of more than 10 Me, but also to smaller companies in a member state if they provide essential and crucial services or are part of critical-strategic Supply Chain





Thank you!

gordionet.com

Rome - Italy

andrea.bucciarelli@gordionet.com
+39 3356414657

All contents are extrapolated from Market-Business Analysis/Intelligence performed by Gordionet and/or from Gordionet's direct involvement in Space Sector/Economy projects. The contents are not confidential and are not covered by NDAs

ICT/TLC/Digital Integration - Digital Transformation - Outsourcing Services Gordionet Business Agency Special skills in Satellite Sector/Economy with Surveys - Market-Business Analysis/Intelligence - Business Development - Marketing & Sales - Go-to-Market - ESA bidding/tendering - Project Management