Protecting the Satellites

Mains: *GS III – Science and Technology- Space Technology*

Why in News?

Recently, Indian government has approved a ₹27,000-crore programme to launch about 52 new surveillance satellites, with the first expected in 2026.

What are satellites?

- **Satellites** – Satellites are celestial bodies or man-made objects that orbit a larger body, such as a planet or star.
- **Types** – There are two main types
  - **Natural satellites** – This includes Earth's Moon, which orbit planets
  - **Artificial satellites** – Human-made objects launched into orbit for various purposes like communication, navigation (GPS), weather monitoring, and scientific research
- **Uses** – Satellites today guide airplanes and ships, power the internet, television services, and global financial transactions, and help scientists monitor the weather and climate change.
- They are also indispensable for national security as contemporary armies depend on satellites for communications, surveillance, and navigation.
- **Bodyguard satellites** – It is also known as surveillance satellites.
- They are dedicated spacecraft designed to escort and protect high-value satellites by monitoring close approaches, detecting threats, and countering hostile manoeuvres in orbit.

What are the risks faced by satellites?

- **Associated risks** – As the number of satellites in orbit has grown, so have the risks.
- Spacecraft can collide with debris, be jammed by radio interference, hacked through ground systems, and threatened by hostile manoeuvres by other satellites.
- **Threat of debris**– Even as a physical environment, space presents risks that would be unimaginable on the ground.
  - **For example**, a small screw left over from a rocket can punch a hole in a spacecraft traveling at 28,000 km per hour, enough to terminate the mission.
- **Risk from transmitters** – Satellites use radio signals to talk to the earth, including with users of navigation services.
- A powerful ground transmitter can jam a satellite's uplink or downlink or use *spoofing.*

Spoofing *is where false signals imitate genuine ones can mislead navigation users.*

- **Natural threats** – Solar storms can damage electronics, induce currents in power systems, and increase atmospheric drag, causing spacecraft to fall out of orbits sooner than expected.
- **Geopolitical threats** – Beyond debris and natural threats also lies the shadow of geopolitics. Satellites can be inspected, shadowed or even targeted by third-party actors.
- Rendezvous and proximity operations used to be a niche technology but have become ubiquitous today.
- While the satellite that allegedly approached the Indian satellite in 2024 didn't result in a collision, officials are said to be reading it as a test of capability and a warning.

What are the measures taken by various countries?

- **Managing debris risk** – To manage this risk, International organisations and countries have built large debris-tracking networks.
    - **UN** – The UN Committee on the Peaceful Uses of Outer Space (COPUOS) adopted voluntary guidelines in 2019 for the long-term sustainability of space.
    - **NATO** – It has declared space to be an operational domain, and have come together under the Combined Space Operations Initiative to promote responsible behaviour in orbit.
    - **US** – The US operates the Space Fence, a radar that can spot objects the size of a marble.
    - **EU** – The European Union runs EU Space Surveillance and Tracking (EUSST), which warns satellite operators about impending threats.
    - **India –** India has the Indian Space Situational Awareness and Management (IS4OM) centre in Bengaluru.
    - It is a satellite-tracking hub that tracks satellites, warns of dangerous encounters, and coordinates collision avoidance manoeuvres.
    - Indeed, in 2023 alone, Indian satellites executed more than 10 collision-avoidance manoeuvres.
    - In 2024, India hosted the Inter-Agency Debris Coordination Committee (IADC), where ISRO publicly declared its intention to pursue 'Debris-Free Space Missions by 2030'.
    - **Project NETRA** – India's Project NETRA is expanding these capabilities with new radars and telescopes.
    - The Multi-Object Tracking Radar at Sriharikota already provides some coverage while some new sites around the country are in the works.
- **Combating cyber threats** - Agencies worldwide issued advisories and set up partnerships.
    - **US** – The US has the Space Information Sharing and Analysis Centre (ISAC) to coordinate cyber threat intelligence.
    - Spacefaring agencies have responded to such threats by designing hardened waveforms and systems.

    - **For instance,** the US military developed its 'Protected Tactical Waveform' for anti-jam communications and 'Advanced Extremely High Frequency' satellites that use frequencies that are harder to disrupt.
  - The US is also deploying an encrypted GPS M-code.
  - **Europe** – It has rolled out Galileo OSNMA, which authenticates navigation messages to minimise spoofing.
  - **India** – With the use of NavIC, The Indian Space Research Organisation (ISRO) has been testing Navigation Message Authentication (NMA).

Navigation Message Authentication (NMA), *is a system that will allow receivers to verify that signals are the real deal.*

  - India's CERT-In has issued guidelines for satellite operators that emphasise strong encryption, network segmentation, secure credentials, regular patching, and incident reporting.
  - India's new licensing framework through IN-SPACe also requires private operators to comply with safety and security standards.
- **Protecting from solar flares** – India also took a major step with the Aditya-L1 mission, launched to study the sun from the L1 Lagrange point.
- Data from this mission can yield early warning of coronal mass ejections and other solar activity.
- This helps satellite-controllers place spacecraft in safe mode and/or plan orbital manoeuvres that minimise exposure.

What can be the potentials of bodyguard satellites?

- **Positioning** – These spacecraft could be positioned near a critical satellite to monitor its surroundings.
- **Detection and warning** – It can detect suspicious manoeuvres by other satellites, warn of threats, and physically intervene if required.
- **Supports orbital assets** – They may also accompany orbital assets that protect against suspicious approaches.

- **Protection from hostile actions –** It act as a shield against anti-satellite (ASAT) weapons or hostile spacecraft.
- It can intercept or disable enemy satellites that try to approach or tamper with the protected satellite.
- **Inspection and repair –** It can move close to the main satellite to check for damages, malfunctions, or tampering.
- **Backup functions –** It can take over communication or navigation services if the main satellite fails.

What needs to be done?

- **Continuous monitoring** – Constant monitoring and signals must be encrypted, networks must be segmented to avoid threats from various sources.
- **Framing clear rules** – Clear and strict international rules could play an important role in protecting the satellites.
- **Ensuring re-entry** – Once a satellite has neared the end of its life, finally, operators need to ensure controlled re-entry and passivation, or adhere to restrictions on how long dead spacecraft can remain in orbit.

What lies ahead?

- In the final analysis, protecting satellites is no small feat — but the benefits have increasingly outweighed the expenses.

Reference

The Hindu| Protecting Our Satellites

SHANKAR
IAS PARLIAMENT
Information is Empowering