Modern Space Warfare and Orbital Cyber Vulnerabilities

Mains – *GS III – Security and Technology.*

Why in News?

Recently, The U.S. Space Force confirmed the deployment of operational "on-orbit space control weapons" to defend space assets against hostile actions.

What are On-orbit space control weapons and how does it impact in space warfare?

- **Space warfare –** Combat or military operations that happen in, or directed at outer space to destroy enemy's space assets.
- **On-orbit space control weapons –** They are military systems placed into Earth's orbit that use kinetic or non-kinetic means to disrupt, degrade, defend, or destroy adversary space capabilities.
- **Kinetic method –** Physical destruction of a satellite or target using direct-ascent missiles or high-speed impactors, which often creates long-lasting space debris.
- **Non-Kinetic method –** Reversible or non-destructive methods including radio-frequency jamming, cyberattacks against ground control, laser dazzling, and signal spoofing.
- **Impact** – Modern space warfare has moved away from physical missiles that blow up satellites to **silent cyber-attacks and signal disruptions**.
- This change makes it harder to separate civilian infrastructure from military targets.

How is the nature of orbital conflict changing, and what key tools are deployed in modern space warfare?

- Old space conflicts focused on kinetic strikes that caused physical damage and created dangerous space debris.
- Modern counter-space warfare uses soft-kill methods that leave no physical trace but can completely disable systems.
- **Three tools of cyber-space interference**

    - **Jamming –** Blocking signals between satellites and the ground to stop communication.
    - **Spoofing –** Sending fake signals to deceive navigation and flight systems.
    - **Ground Station Hacking –** Hacking earth-based control centers to hijack satellite functions.
- **Result –** An attacker does not need to destroy a satellite physically. Using malware to turn a satellite into a non-working object ("bricking" it) produces the same military result as blowing it up.

What are the main legal and strategic challenges?

- **International law facing a legal blind spot –** The **UN Charter (Article 2(4))** bans the threat or use of force.
- However, it does not clearly define whether a non-physical cyber-attack counts as a use of force.
- **Shift to an effects-based test –** Experts now support an *effects-based test*.
- If a cyber-attack disables satellites supporting power grids or banking, the real-world impact is identical to a missile strike, so it should be treated as a use of force.

What is the attribution gap and why does it weaken deterrence?

- **Strategic anonymity –** Attackers route cyber operations through proxy networks and spoofed identities, leaving no physical evidence behind.
- **Proof problem –** Under the **International Law Commission (ILC)** rules, holding a nation legally responsible requires high evidentiary certainty.
- Because digital attacks leave little visible proof, aggressors can attack without fear of clear retaliation.

Why is the civilian-military divide collapsing?

- **Dual-use satellites – International Humanitarian Law (IHL)** and the **Outer Space Treaty (1967)** state that militaries must separate civilian assets from military targets.
- **The Starlink Precedent –** Private satellite constellations now offer "space-as-a-service" directly to military operations for drone targeting and communication.
- Because civilian networks help military kill-chains, they lose their civilian

legal protection and become targets in grey-zone conflicts.

How does orbital dependency threaten the Global South?

- **Third-party reliance –** Developing economies rely heavily on foreign commercial satellites for banking, emergency response, and government digital networks.
- **Impact on states –** A single silent strike on a private satellite operator can shut down a developing country's economy, government functions, and military visibility without a single shot being fired.

Where does India stand on space security?

Strategic Area	Current Policy & Action	Operational Gap
Policy Standard	**2026 CERT-In / SIA-India Guidelines**	Requires a **"Secure-by-Design"** framework for satellites across their entire lifecycle (design, launch, operation, and decommissioning).
Military Capability	**Defence Space Agency (DSA)**	Formed to integrate armed forces space assets and handle counter-space threats.
Main Vulnerability	**Real-time Attribution**	India is expanding its satellites faster than its ability to track and identify cyberattacks in real time.

What lies ahead?

- **Clear international rules –** Turn vague guidelines into strict rules that clearly classify cyber-paralysis of satellites as a violation of UN Charter Article 2(4).
- **Shared attack-tracing systems –** Build international platforms to trace and identify cyberattacks on space systems quickly to fix the attribution gap.
- **Secured satellites –** Enforce "secure-by-design" practices globally, including stronger signal encryption and backup systems in orbit.
- **India's strategic autonomy –** Expand local constellations (like NavIC) and build secure domestic satellites to reduce reliance on third-party networks.

Reference

[The Hindu | On-orbit space control weapons]

SHANKAR
IAS PARLIAMENT
Information is Empowering