

33rd UN/IAF Workshop · IAC 2026

Emerging Challenges for International Law

AI-Driven Cyber Architectures in Cislunar Space

Space Economy Opportunities for Emerging Nations
Advancing Socio-Economic Resilience through Space Technologies
and Applications

Antalya, Türkiye · 3–4 October 2026

Dr. Nebile Pelin Manti
Istanbul University Faculty of Law
Public International Law Department



Cislunar Space Economy: Architecture of Dependency

UN/IAF Workshop · IAC 2026 · Antalya

The economic layer depends on communication, navigation, data and trust.

Cislunar economy is a distributed network of cyber-physical dependencies.

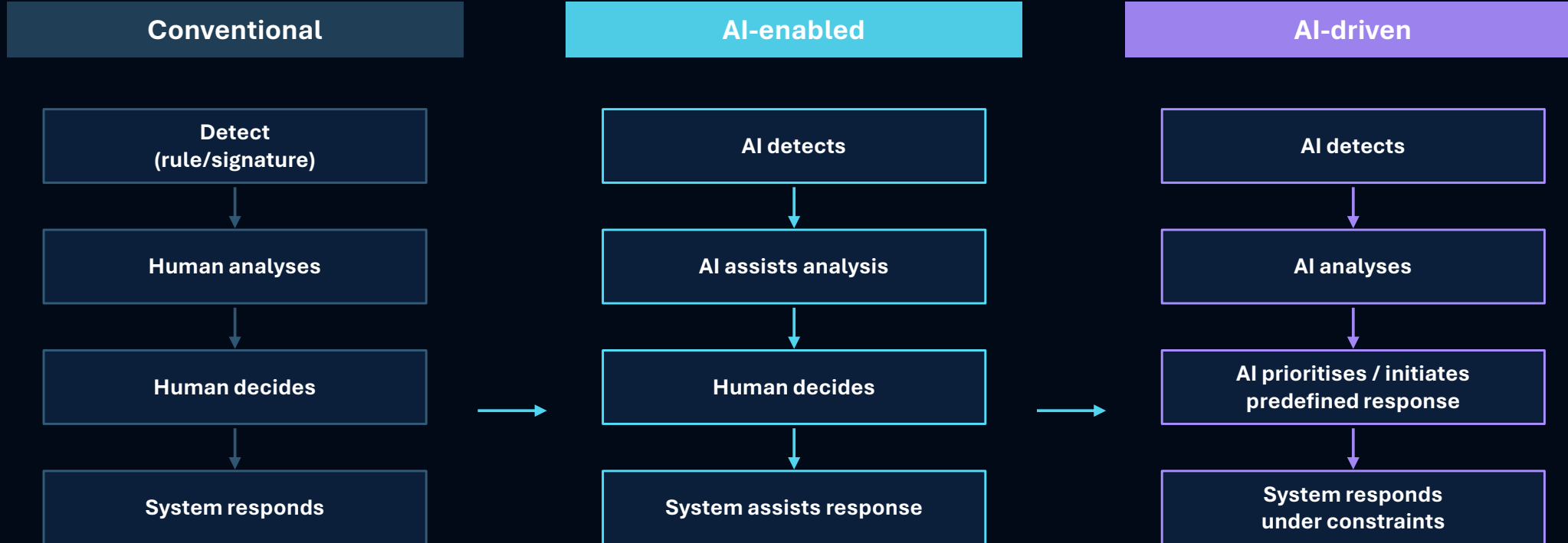
- Lunar operations depend on relay nodes, data links and autonomous coordination
- Economic opportunity depends on reliable access to digital infrastructure
- Cyber disruption can affect physical, economic and legal continuity

**Dependency is no longer only physical or financial.
It is cyber-operational.**



Why AI-Driven?

The key change is the location and tempo of operational decision-making.



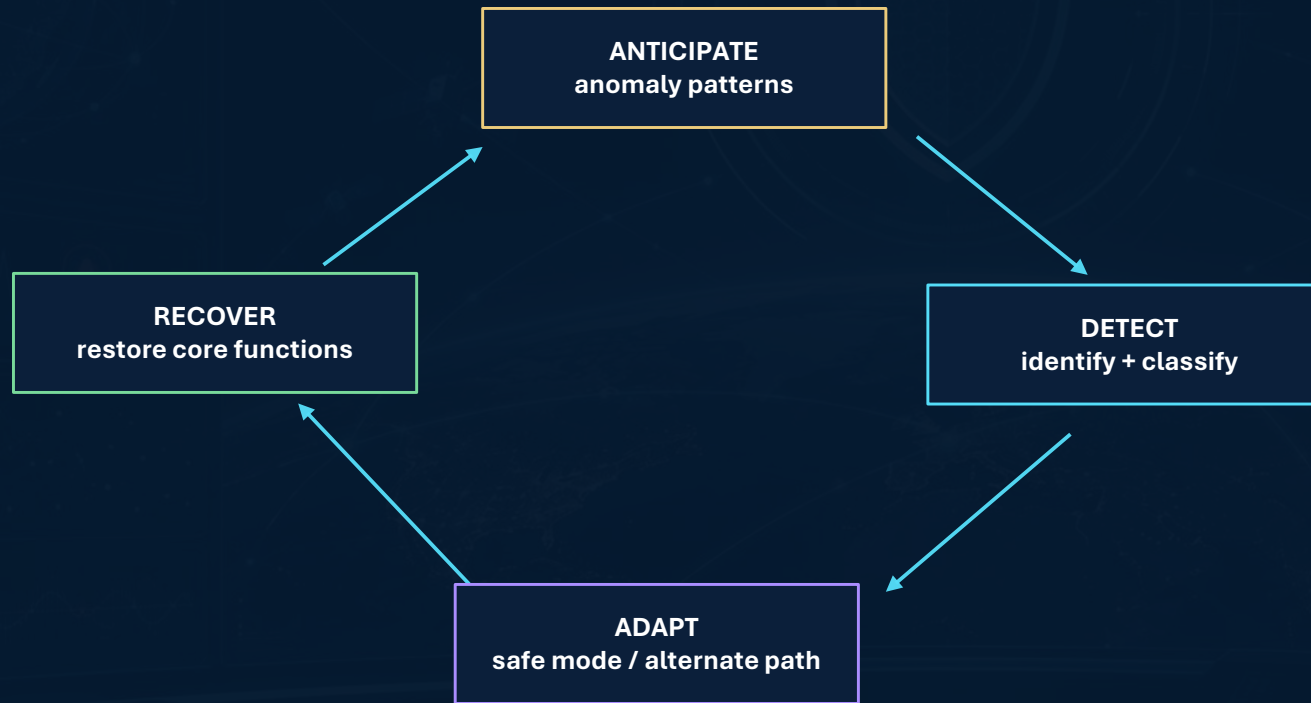
In cislunar space, autonomy responds to distance, latency and intermittent connectivity — not merely convenience.

AI and Resilience: Anticipate · Detect · Adapt · Recover

UN/IAF Workshop · IAC 2026 · Antalya

Cybersecurity becomes part of socio-economic resilience.

Operational resilience cycle



AI can help maintain continuity when real-time human intervention is delayed or unavailable.

Legal relevance

The same system that strengthens resilience also raises questions of supervision, foreseeability, traceability and review.

Resilience is not simply prevention; it is continuity under disruption.

International Law + Space Law Framework

UN/IAF Workshop · IAC 2026 · Antalya

The legal challenge arises at the intersection of two normative architectures.

International Space Law

- Outer Space Treaty
- Article VI: authorization and continuing supervision
- Article VII: liability
- Article IX: due regard and harmful interference

Cislunar Cyber Operations

AI-driven systems monitor, classify and respond within cyber-physical space infrastructures.

Legal challenge: preserving traceability and review while enabling resilience.

International Law / Cyber Norms

- Attribution
- State responsibility
- Due diligence
- Non-intervention / use of force thresholds
- Cooperation

The question is not whether law applies, but how obligations are operationalised in autonomous cyber architectures.

Attribution, State Responsibility and Due Diligence

UN/IAF Workshop · IAC 2026 · Antalya

Three legal questions created by AI-driven cyber architectures.

01 ATTRIBUTION

Who acted?

How should conduct be characterised when AI systems autonomously detect, classify and trigger cyber responses?

02 STATE RESPONSIBILITY

Who is responsible?

Public, private or mixed deployment does not remove responsibility when systems are authorised, supervised or controlled by States.

03 DUE DILIGENCE

What should have been prevented?

What level of supervision, precaution, traceability and review is required to prevent foreseeable harm?

AI does not become a legal actor. Responsibility remains with States and other legal persons under international law.

Emerging Nations: Resilience as Access

UN/IAF Workshop · IAC 2026 · Antalya

Cyber resilience becomes part of access, trust and capacity-building in the space economy.

Main claim

For emerging nations, cybersecurity is not merely a technical add-on. It is becoming a condition of meaningful participation in the cislunar economy.

Risks to inclusion

- dependency on externally controlled infrastructures
- lack of access to secure data and trusted services
- asymmetric exposure to disruption, liability and compliance costs

Capacity-building must include legal resilience + cyber resilience from the outset.

Access pathway

access

trust

capacity

resilience

Selected References

UN/IAF Workshop · IAC 2026 · Antalya

Sources supporting the legal and workshop framing.

UN/IAF Workshop

33rd UN/IAF Workshop on Space Economy Opportunities for Emerging Nations, Antalya, 3–4 October 2026.

Outer Space Treaty

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, Arts VI, VII and IX.

IISL AI Report

IISL Working Group on Legal Aspects of AI in Space, Balancing Innovation and Responsibility: International Recommendations for AI Regulation in Space (2024).

Cyber law

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations; State practice and UN processes on responsible State behaviour in cyberspace.

Cislunar governance

Recent literature on cislunar space domain awareness, relay architectures, lunar infrastructure and space economy participation.

Core message: AI may increase cislunar resilience, but international law must preserve attribution, responsibility, due diligence and equitable participation.