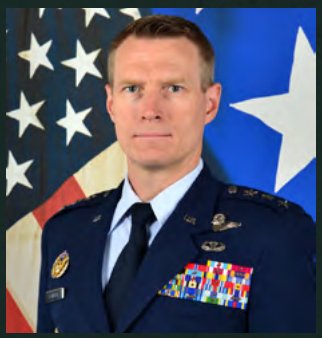
WHEN SPACE GOES DARK :

THE NEW FRONTLINE OF STRATEGIC PARALYSIS

INTERVIEW QUESTIONS
-LIEUTENANT GENERAL (RET.) LANCE LANDRUM



Lieutenant General Lance Landrum served more than 31 years in the U.S. Air Force, developing deep expertise in joint and combined operations, ISR, and capability development. As NATO's Deputy Chair of the Military Committee, he played a vital role in shaping Allied consensus during a period of heightened geopolitical tension. He previously served as Director of Operations at U.S. European Command and as Deputy Director for Requirements and Capability Development on the Joint Staff, where he helped validate service-led capability programmes against joint requirements. He now leads Team Landrum Advising & Consulting LLC and serves as a Senior Fellow at the Centre for European Policy Analysis.

Hosted by ideas Strategic Insight for Defense and Security

In partnership with ST Engineering

Powered by ABLO CONSULTING

1. If GNSS or SATCOM were degraded for a week, which civilian and military systems would fail first and how should we prioritise responses?

A week-long degradation of Global Navigation Satellite Systems (GNSS) or Satellite Communications (SATCOM) would trigger a series of failures across both civilian and military systems. In the civilian sector, systems relying on high-precision timing and real-time connectivity would fail first. The financial sector, especially precise high-frequency trading and critical banking operations that rely on GNSS timing for transaction synchronization, would immediately suffer instability, leading to potential market halts and significant economic disruption. Similarly, critical infrastructure control systems, including power grids and telecommunications networks, like cellular towers using GNSS for synchronization, would quickly lose cohesion, resulting in widespread service outages. Transportation systems, particularly commercial aviation, which heavily relies on satellite navigation signals for both enroute legs and precision landing procedures through poor weather would immediately and significantly impact commercial aviation. Additionally, if maritime shipping lost both navigation and SATCOM, the industry would face immediate operational bottlenecks due to loss of command and control and clogged port entry/exit and scheduling processes.

For military forces, the initial failures would concentrate on networked and precision-guided systems. Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems, which are heavily reliant on SATCOM for beyond-line-of-sight communication and GNSS for positioning and autonomous operations, would be quickly degraded. This would reduce situational awareness and compromise the ability to coordinate dispersed units. Furthermore, precision-guided munitions and cruise missiles that depend on GNSS for navigation and terminal guidance would be rendered ineffective. Units operating in remote areas without robust terrestrial or legacy communication backups would become isolated. While inertial navigation systems would provide temporary positioning, gyroscopic systems would drift over time, reducing accuracy, especially if there are a lack of procedures and techniques to correct the navigation errors.

The response to such failures should be incorporated into a broader national resilience effort which should include maintaining civil order, preserving critical infrastructure, and ensuring enough credible military capability to deter further aggression and defeat any opportunistic adversary. The civilian sector domain must stabilize the power grid and telecommunications networks, possibly through manual operation and activation of terrestrial synchronization methods, like atomic clocks or existing fiber networks, to prevent total collapse. Additionally, restoring basic air traffic control and maritime safety communication via non-satellite-dependent systems, like VHF Omnidirectional Range, Instrument Landing Systems, HF radio, landlines connections, and manual port operations, etc., would be essential. In the military domain, establishing and using pre-planned continuity of operations plans would be the first step. This could involve activating secure, non-SATCOM dependent communications protocols (e.g., frequency hopping HF/VHF/UHF radio, messenger services) and shifting from precision strikes to area targeting or reliance on terrain-aided navigation and legacy guidance systems. Long-term efforts should focus on deploying mobile alternative positioning, navigation, and timing systems and strengthening hardened fiber-optic networks.

2. What is the fastest, most affordable mix of C-PNT, nano-constellations, and hardened SATCOM NATO–EU could realistically deploy in 12–24 months?

Considering the 12–24 month timeline in the question, the fastest and most affordable mix for NATO-EU C-PNT, nano-constellations, and hardened SATCOM should prioritize commercial off-the-shelf technology, strategic partnerships, and focused terrestrial enhancements over developing entirely new space assets. The NATO Commercial Space Strategy endeavors to increase understanding and access to commercial space opportunities to leverage the capacity of creativity of industry.

For C-PNT, the most immediate solution involves hardening existing infrastructure and augmenting it with terrestrial and low-Earth orbit commercial services. This means rapidly deploying COTS alternative PNT systems, such as enhanced inertial navigation systems and terrestrial radio-frequency sources integrated with military-grade GNSS receivers featuring enhanced anti-jamming and anti-spoofing capabilities. Simultaneously, rapid integration of secure timing signals derived from commercial LEO satellite constellations (like those from Starlink, OneWeb, or specialized providers) can offer affordable redundancy for timing.

In terms of nano-constellations and hardened SATCOM, the focus should be on leveraging existing or near-ready commercial LEO and Medium Earth Orbit assets, particularly those with proven security and high throughput. Governments must ensure contractual arrangements are very strong to allow for access and use during crisis and conflict. One approach could be to invest in rapidly deployable, secure user terminals and network infrastructure to access resilient commercial SATCOM networks. This includes procuring numerous dual-band/multi-orbit user terminals (UHF/Ka/X-band) and establishing a secure network overlay that routes essential command and control traffic across multiple, diverse commercial constellations.

3.How can we build attribution systems and intelligence-sharing processes that produce legally and operationally credible findings within hours/days?

Attribution in the context of hybrid warfare against space assets faces significant technical and political hurdles. To achieve legally and operationally credible findings within hours or days, an immediate and multi-layered approach is required. Technically, this necessitates integrating advanced sensor networks—both terrestrial and space-based—with AI-driven analytics capable of processing massive data streams in near real-time. These systems must correlate telemetry, cyber signatures, and physical evidence (such as debris analysis or jamming patterns) across multiple domains. Crucially, the system must be designed from the outset to preserve a chain of custody for all data, meeting international legal standards for evidence admissibility and ensuring that the analytical output clearly distinguishes between technical possibility and legal certainty.

Operationally and legally credible attribution depends heavily on robust, pre-negotiated intelligence-sharing protocols. Instead of waiting for a crisis, allied nations and commercial operators must establish standardized, automated sharing pipelines for anomaly detection and raw data. These agreements need to define what constitutes a "reportable event" and mandate immediate, trusted sharing across a dedicated, secure network. Furthermore, a permanent, multi-national body composed of technical, legal, and military experts should be empowered to rapidly synthesize shared intelligence, apply common forensic standards, and issue provisional findings. This body must operate under a clear legal framework that establishes thresholds for escalating findings from "likely" to "actionable" attribution, ensuring that rapid reporting does not sacrifice evidentiary rigor.

Ultimately, the credibility of rapid attribution rests on institutionalizing resilience and transparency. This means developing and sharing common baselines of expected activity for space assets to immediately flag deviations, and investing in forensic capabilities designed specifically for the unique environment of space. By proactively formalizing the legal standards for space-related evidence, synchronizing national cyber and space defense intelligence streams, and practicing joint attribution drills, the international community can move toward a system where rapid, high-confidence findings are the norm. This shift transforms attribution from a reactive investigation into an integrated, near-real-time component of hybrid deterrence.

4.What incident-response playbooks and information-sharing mechanisms should NATO and the EU put in place now to coordinate cross-sector recovery?

To effectively preserve space superiority against a spectrum of adversary hybrid actions, from peace to conflict, NATO and the EU must urgently develop shared incident-response playbooks and robust information-sharing mechanisms. In the context of developing a range of potential responses, the work must be done in the context of difficult consultation processes during times of stress and crisis, both inside the NATO Alliance and in coordination with the EU. Part of the work must be lean on the agreed foundation that NATO is the single security forum for the transatlantic area.

The initial step requires creating standardized, tiered playbooks that clearly define pre-agreed triggers, escalation protocols, and roles for responding to space-related incidents impacting critical terrestrial services. These playbooks must address scenarios ranging from subtle GPS jamming (peace/crisis) to kinetic or high-energy directed energy attacks on satellites (conflict), ensuring seamless integration of military and civil responses across communications, energy, financial, and transportation sectors. Specific attention must be paid to 'grey zone' actions where attribution is difficult, necessitating shared forensic procedures and legal frameworks for collective defense activation.

The second component is establishing an operational high-speed information-sharing architecture. This mechanism should go beyond current bilateral arrangements to include a unified fusion center capable of synthesizing intelligence from NATO's military assets and the EU's civil/commercial space monitoring centers, such as the EU Space Surveillance and Tracking network. This platform needs to facilitate the rapid exchange of real-time situational awareness, threat assessments, and, crucially, damage reports required for coordinated recovery efforts. A dedicated, classified channel for sharing commercial satellite operator data—protected by agreed-upon legal immunities—would be essential for minimizing downtime following an attack.

Finally, the coordination strategy must be solidified through regular, joint, full-spectrum exercises that test these playbooks and sharing mechanisms. These exercises, which must involve both military and civilian leadership alongside key private-sector partners (telecom, finance, space operators), should focus specifically on post-incident recovery processes, including orbital debris mitigation, temporary service restoration using backup constellations, and coordinated public messaging to maintain stability. By institutionalizing these comprehensive, cross-sector recovery protocols now, NATO and the EU can ensure that an adversary's attempt to degrade space superiority does not translate into prolonged, uncoordinated systemic failure across the Euro-Atlantic area.

5. How must procurement rules, insurance models, and commercial contracts change so private satellite operators can surge resilience capabilities under Alliance direction?

NATO's embrace of a commercial space strategy necessitates a fundamental overhaul of procurement regulations, risk management frameworks, and contractual agreements to effectively integrate private satellite operators as Alliance resilience partners. Procurement rules must shift from rigid, traditional defense acquisition models to agile, rapid contracting mechanisms that can leverage existing commercial capabilities. This means establishing pre-negotiated service agreements that define service levels, security protocols, and intellectual property rights in advance of any crisis. Furthermore, procurement must prioritize capability-based purchasing rather than platform-specific ownership, allowing NATO to quickly task commercial assets like high-throughput communications, Earth observation, or sophisticated data analytics when needed.

The existing insurance and liability models are ill-suited for the dynamic, high-stakes environment of crisis surge support under Alliance direction. Traditional commercial space insurance typically excludes acts of war or military engagement, a gap that must be addressed through new, specialized risk-sharing instruments. NATO should explore creating a sovereign-backed insurance or indemnification fund that covers commercial operators when their assets are tasked for Alliance missions, particularly if they face increased risk exposure from hostile action. Concurrently, new liability models are required that clearly delineate responsibility between the Alliance and the private operator during directed missions, ensuring that the burden of increased risk for critical national or NATO security support does not fall solely on the commercial entity. Still, industry must step up their side of risk tolerance in today's unpredictable security environment, and those companies that do stand to gain from the current commercial opportunities at hand.

Finally, commercial contracts must evolve to contain robust, clearly defined "surge clauses" that formalize the process for Alliance tasking of private assets during a crisis. These clauses must address security requirements, including immediate implementation of Alliance-mandated cybersecurity and physical protection measures for sensitive data and operations, as well as clear protocols for command, control, and de-confliction. The contracts must also establish transparent and equitable compensation structures that incentivize operators to maintain excess capacity and prioritize Alliance requirements during times of high demand. This contractual framework must ensure seamless, legally sound, and timely transition from purely commercial operations to mission-specific support under NATO direction, thereby translating the commercial strategy into genuine operational resilience. In the end, NATO must ensure the Alliance has access to the capabilities it needs when it needs them. The Alliance cannot allow itself to be held hostage by industry in times of crisis and conflict.

6. What transparency or confidence-building measures could reduce miscalculation while legal regimes mature?

The most immediate transparency and confidence-building measures should focus on sharing operational data and establishing open lines of communication regarding threats, anomalies, on-orbit maneuvers and satellite status. This involves governments and commercial operators collaboratively participating in standardized Space Situational Awareness data sharing protocols, potentially managed by an agreed multi-national consortium. By providing near real-time, accurate orbital information, including planned or recent changes, operators reduce the likelihood of misunderstanding or miscalculation and mitigate the risk of one party misinterpreting a standard operational movement as an aggressive act or an impending failure.

Another way centers on agreed-upon norms of behavior in key operational areas, even before formal legal frameworks are enacted. This includes establishing "keep-out zones" or self-imposed safety corridors around high-value or highly sensitive assets, with the clear commitment to notify all parties of incursions or proximity operations. Furthermore, an agreement to openly communicate the purpose of dual-use satellite launches (e.g., whether a mission is purely commercial, research-oriented, or possesses a military capability) could significantly de-escalate potential misunderstandings, fostering a shared understanding of the space environment and the intent behind various operations.

Finally, regularized, dedicated bilateral and multilateral forums that include both government and commercial sector representatives are essential. These forums should be non-attributive, focusing on technical discussions regarding anomalies, best practices for debris mitigation, and early warning for space weather events. By institutionalizing channels for technical dialogue, these measures create a foundation of trust. This technical cooperation will, in turn, provide practical, real-world experience that can directly inform and accelerate the development of robust, consensus-driven legal regimes appropriate for the rapidly evolving hybrid space domain.

View an in-depth panel discussion on
When Space Goes Dark : The New Frontline of Strategic Paralysis

CLICK HERE

EUROSATORY
PROTECT YOUR FUTURE

15-19 JUNE 2026, PARIS

WWW.EUROSATORY.COM

Hosted by ideas Strategic Insight for Defense and Security

In partnership with ST Engineering

Powered by ABLO CONSULTING