G1VE TECHNOLOGIES

When GPS Goes Dark: The Jamming Age Is Coming for Civil Aviation, Logistics, and Joint Force Command

W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP

Apr 20, 2026

Original source

https://www.linkedin.com/pulse/when-gps-goes-dark-jamming-age-coming-civil-aviation-w-b--s4zxc/

I. GPS Is No longer Just A Convenience — It Is National Infrastructure

Most Americans think of GPS as a navigation utility. Defense planners know better. Position, navigation, and timing — PNT — is foundational infrastructure. Center for Strategic and International Studies (CSIS) notes that GPS timing supports the internet, cell phone networks, and credit card transactions, while emergency responders, buses, trains, planes, and ships rely on PNT to get to the right place at the right time. Center for Strategic and International Studies (CSIS) also cites a 2019 estimate placing GPS's cumulative value to the U.S. economy at $1.4 trillion since the 1980s.

That means GPS disruption is not just a transportation problem or a military problem. It is a national continuity problem. It touches finance, telecom, emergency response, logistics, and force projection. In a crisis, those functions do not fail neatly by sector. They degrade together.

The strategic hazard is that the United States has become deeply dependent on GPS while shedding much of the terrestrial backup architecture it once possessed. Center for Strategic and International Studies (CSIS) argues that the country is now "clearly over reliant" and in many ways "wholly dependent" on GPS for PNT services. In an era of great-power competition, that is not merely inefficient. It is exploitable.

II. Jamming Is Spreading Because It Is Cheap, Deniable, and Effective

Breaking Defense reported in April that the Secure World Foundation 's latest counterspace assessment found 13 nations have developed or are developing counterspace capabilities, with Germany newly added as the 13th. The report also highlighted growing use of radio-frequency jamming against GPS and other PNT satellites, alongside jamming of satellite communications.

That trend should not surprise anyone in the defense community. Jamming is attractive because it is scalable, comparatively low-cost, often reversible, and frequently ambiguous below the threshold of open warfare. It allows adversaries to create confusion without immediately crossing into overt destructive attack. It can disrupt military users, civil users, or both. It can be episodic, geographically limited, or campaign-based.

Breaking Defense notes that the European Commission has publicly criticized Russia for GPS jamming in the Baltics due to effects on civilian aviation, and the International Telecommunication Union has condemned both Russia and North Korea for peacetime satellite jamming. The same report points to Russian experience using sophisticated ground-based jammers, persistent Iranian interference with commercial satellite signals and STARLINK terminals, and North Korean ability to jam civilian and military GPS in limited areas.

The operational lesson is brutally simple: if an adversary wants to create friction in the U.S. or allied decision cycle, GPS disruption is one of the fastest ways to do it.

III. The True Target Is The Civil-Military Seam

The Federal Aviation Administration 's airport GPS disruption best-practices document is one of the clearest public illustrations of why this matters. It warns that GPS disruptions can affect

safety, efficiency, security, and regulatory compliance, and that impacts may extend beyond aviation into communications, multiple transportation modes, emergency response, utility services including power, water, and natural gas, inventory and warehousing systems, and even financial transactions.

That is the heart of the matter. The target is not just the airplane, the satellite, or the ship. The target is the interdependency layer: the seam where civil infrastructure and military operations rely on the same timing and navigation fabric.

A port that cannot synchronize operations cleanly does not just suffer commercial delay. It slows military sealift options. An airport managing disruption does not just inconvenience passengers. It strains emergency management, scheduling, and downstream cargo flows. A timing disturbance inside telecom or financial infrastructure can ripple into command, logistics, and public confidence. Mission assurance is therefore inseparable from infrastructure assurance.

IV. US Congress Is signaling that resilience cannot wait

Breaking Defense reported that appropriators directed $30 million for United States Department of War to develop an integrated PNT architecture using a Modular Open Mission Systems approach, while also ordering a written plan of action and milestones for more resilient capabilities across space, ground, and user-equipment segments.

That same reporting notes that current GPS III satellites bring up to eight times the jam resistance of earlier variants, while Lockheed Martin said GPS IIIF's Regional Military Protection signal will provide more than 60 times the anti-jamming capability of legacy GPS satellites. Starting with SV13, GPS IIIF satellites are also expected to use the cyber-hardened LM2100 Combat Bus to strengthen resiliency.

Those improvements matter. But the same article also makes clear that lawmakers are dissatisfied with the pace, particularly with delays and the termination of the Resilient-GPS program in the FY26 request. The message from US Congress is unmistakable: modernization of the space layer is necessary, but not sufficient. Resilience requires a broader architecture.

Center for Strategic and International Studies (CSIS) makes the same point more directly, arguing that true resilience requires a combined space and terrestrial architecture with no common dependencies, rather than continued reliance on space alone.

V. What Preparedness Looks Like In Practice

The Federal Aviation Administration 's five-step airport resiliency framework is useful far beyond airports. It recommends:

1. Education and familiarization;
2. Inventory and assessment of GPS dependencies;
3. operational response development;
4. Response integration across stakeholders; and,
5. Policy and procedure development.

That structure is directly applicable to ports, energy operators, telecoms, defense contractors, state emergency managers, and military installations.

A serious PNT resilience program should identify which systems fail gracefully, which fail dangerously, and which fail silently. It should distinguish between functions that require full backup and those that can tolerate degraded performance. It should establish reporting mechanisms, escalation thresholds, manual workarounds, and joint coordination channels. Most of all, it should force leaders to confront an uncomfortable reality: dependency hidden inside routine operations is still dependency.

This is where doctrine, procurement, and operations meet. If organizations do not understand their timing and navigation dependencies now, they will learn them during a disruption event — which is the most expensive way possible.

VI. The Deterrence Issue

Resilience is not only about continuity. It is also about deterrence. If adversaries believe GPS disruption can impose outsized cost on U.S. and allied systems, they have incentive to use it. If, on the other hand, the United States builds layered resilience across satellites, terrestrial timing, commercial alternatives, user equipment, doctrine, and exercises, the value of the attack falls.

Center for Strategic and International Studies (CSIS) argues precisely this point: a layered national PNT architecture would both strengthen deterrence and reduce the attractiveness of attacks against the space layer in the first place.

That is the correct frame. The goal is not perfect immunity. The goal is to make disruption operationally unprofitable.

VII. Bottom line

When GPS goes dark, the first effects may appear technical, but the real consequences are strategic. Aviation safety, telecom timing, emergency response, logistics coordination, port operations, financial synchronization, and military command all sit downstream of PNT resilience. The jamming age is here because the attack vector is efficient, deniable, and consequential. The answer is not panic. The answer is architecture: layered resilience, interagency governance, backup timing, hardened user equipment, and mission rehearsals that assume degradation is coming.

✨ Call to Action: Step Into the Arena ✨

Most professionals will read about the future. A select few will shape it.

If you are serious about staying ahead of the curve in Artificial Intelligence, Regulatory Compliance, and Enterprise Risk, this is where you need to be.

📩 Subscribe to Securing Our Futureto gain direct access to:

1. Strategic foresight on AI Governance & Ethical Deployment
2. Real-world applications across National Security & Mission Assurance
3. Advanced GRC, TPRM, and Regulatory Compliance frameworks
4. Emerging Fintech and Risk Intelligence innovations

⚔️ The landscape is shifting—fast. The gap between those who understand and those who execute is widening.

This is built for professionals responsible for decisions that carry consequence—not commentary.

📅 Ready to operationalize these insights and move beyond theory?

👉 https://calendly.com/g1ve-technologies

Let us translate insight into measurable, defensible outcomes—and build capability, not just conversation.

🔍 About the Author

W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP is a National Security-aligned Artificial Intelligence Strategist/Tactician and Governance, Risk, and Compliance (GRC) Authority/Subject Matter Expert with over a decade of experience operating at the intersection of National Security, National Defense, Critical Infrastructure, Cybersecurity, AI Governance, Mission Assurance, Mission-Critical Systems, and Predictive Funding/Grant Intelligence.

As Managing Partner at G1VE Technologies, LLC and a Strategic Board Advisor, W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP architects and operationalizes enterprise-scale risk, compliance, and AI governance ecosystems across both Public and Private Sector environments—including Fortune 500/1000 organizations and Federal-aligned missions, where failure is not an option.

His work is centered on delivering Decision Advantage, strengthening Operational Resilience, and enabling organizations to navigate high-stakes, high-uncertainty environments with precision and confidence.

📡 Connect with W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP here to stay at the forefront of:

- Artificial Intelligence
- National Security
- GRC
- Cyber Risk
- Regulatory Strategy
- Mission Assurance