What are the practical barriers to GPS spoofing/jamming countermeasures for critical infrastructure?

April 14, 2026 | SnugLab Research | readme.snuglab.com

Executive Summary

Practical barriers to GPS spoofing and jamming countermeasures for critical infrastructure are primarily economic, technical, and regulatory. The prohibitive expense and technical insufficiency of comprehensive solutions, coupled with the high cost of retrofitting existing systems, represent significant financial hurdles for operators, despite estimated potential economic damages exceeding $100 billion annually from widespread disruptions [1, 8, 14]. Technologically, critical infrastructure's inherent reliance on continuous GPS availability creates a single point of failure, and current detection and mitigation systems are limited [8, 12]. Furthermore, a fragmented regulatory landscape and the lack of enforcement mechanisms by international bodies like the ITU, ICAO, and IMO hinder the establishment of consistent global security standards, making voluntary industry-led approaches insufficient to protect against escalating threats, which impacted over 13,000 vessels in 2025 alone [5, 6, 9, 13].

Key Findings

Economic and Cost-Benefit Challenges

Implementing robust GPS security measures for critical infrastructure faces significant economic barriers, often perceived as outweighing the immediate risk by some operators [1]. Retrofitting existing systems, many of which were designed assuming continuous GPS availability, is particularly cost-prohibitive [8]. The current fragmented approach to security further exacerbates costs, leaving infrastructure vulnerable and expensive to defend [14]. While the potential economic damages from widespread GPS disruptions are estimated to exceed $100 billion annually, with reports suggesting a GPS outage could have an economic impact of "$1 billion a day" for the US economy, these figures are not broken down by sector, hindering targeted investment prioritization [2, 8, 9]. Current risk assessments may also underestimate the true economic cost by not fully accounting for

cascading effects across interconnected critical infrastructure sectors [12]. Despite the high upfront costs, some analyses suggest that a modest initial investment in resilience, such as a 4.6% increase in initial cost, could yield a 35.4% reduction in expected failure costs over a building's life cycle [4]. However, the research does not provide specific 10-year cost projections for deploying alternative PNT systems like eLoran across a representative sample of critical infrastructure facilities [3].

Technical Limitations and Infrastructure Vulnerabilities

"Civil GNSS service is vulnerable to spoofing due to the open structure and low power of GNSS satellite signals," according to one peer-reviewed article [12]. This inherent vulnerability is exacerbated by the fact that "GNSS spoofing is difficult to detect and may result in more serious situations than jamming, since the user may not be aware of it" [12]. Current GPS spoofing and jamming detection and mitigation technologies are limited, primarily focusing on detection rather than full mitigation, due to existing technical and economic barriers [1, 8, 12]. Traditional defense mechanisms, such as multi-antenna systems, are frequently too costly, heavy, or bulky for many applications within critical infrastructure [14]. The increasing accessibility of attack tools, with "open source GPS signal simulators available online and the fast developing software-defined radio technology," makes GNSS spoofing "not only feasible but also affordable" [12].

However, emerging technologies offer pathways to enhance resilience. The High Accuracy and Resiliency Service (HARS) is presented as the most practical and cost-effective pathway to resilient PNT, potentially offering a faster implementation timeline than changes to the core GPS constellation [1]. LEO-based PNT constellations are also considered a viable and scalable solution for mitigating GNSS vulnerabilities, offering improved signal strength and resilience, though they face challenges with initial investment and deployment complexity [10, 13, 15]. While alternative PNT sources like eLoran are considered backup systems, specific cost and deployment details for widespread implementation are not fully specified [1, 8]. Enhanced Inertial Navigation Systems (INS) can offer resilience when GNSS signals are unavailable but require accurate initialization from GNSS and cannot function as standalone solutions for extended periods [1, 13].

Regulatory and Governance Gaps

A significant practical barrier to implementing GPS countermeasures is the fragmented regulatory and governance landscape. International organizations such as the ITU, ICAO, and IMO currently lack sufficient enforcement mechanisms to ensure consistent global GNSS security standards [6]. This deficiency is compounded by the absence of a globally standardized framework for assessing and mitigating PNT-related risk, which hinders effective, cost-justified implementation [8]. Consequently, a voluntary, industry-led approach to GNSS interference mitigation is deemed insufficient to systemically protect critical infrastructure, largely due to asymmetric incentives and the potential for malicious actors to exploit gaps in protection [9, 13].

Moreover, increased operator autonomy in critical infrastructure cybersecurity elevates overall systemic risk by leading to inconsistent security protocols and hindering coordinated defense across decentralized systems [23, 24, 25, 19, 20, 21]. Establishing global GNSS security standards requires specific policy changes and international agreements, including regulatory frameworks, licensing requirements for signal transmission, mandated security standards for GNSS receivers, and clear legal frameworks criminalizing malicious interference [7, 8, 9, 11, 13, 15]. However, the development and deployment of such standards and enforcement mechanisms are expected to take several years [1].

Systemic Risk and Interdependencies

The increasing sophistication of attacks, with state and non-state actors combining cyberattacks with physical disruptions and utilizing AI for faster vulnerability discovery, presents a growing threat to critical infrastructure [5]. Critical infrastructure sectors, including energy, water, communications, and finance, are highly interdependent, meaning a disruption in one sector can lead to cascading failures across others. As one report notes, "A breach in a corporate email system can now be the pivot point to sabotage a water treatment plant or a port crane" [14]. These interdependencies amplify the potential for economic damages, with estimates suggesting a major attack could cost trillions of dollars [23, 24, 25, 19, 20, 21]. Current risk assessments likely underestimate the full economic cost of widespread GNSS disruption because they do not fully account for these cascading effects [12].

There is a debate regarding the most effective approach to securing these interconnected systems. While some argue for prioritizing protection based on criticality as a necessary

strategy within resource constraints [35, 36, 22, 32, 33, 34], evidence suggests that a comprehensive approach to GNSS security, addressing vulnerabilities across all critical systems, is better supported. This is due to the interconnectedness of infrastructure and the potential for cascading failures originating from seemingly less critical points [17, 26, 37, 38, 39, 40]. The Russia-Ukraine conflict serves as a recent example of how GNSS disruption can be weaponized, further highlighting the necessity for proactive, coordinated resilience measures [16].

Implications

The identified practical barriers have significant implications for critical infrastructure protection. The high economic burden of implementing comprehensive GPS countermeasures, coupled with the technical challenges of retrofitting existing systems, means that many operators may continue to prioritize immediate economic concerns over long-term security investments [1, 8]. This creates a persistent vulnerability, especially given the increasing sophistication of attacks and the potential for cascading failures across interdependent sectors, which current risk assessments may underestimate [5, 12]. The lack of a robust global regulatory framework and enforcement mechanisms further compounds this issue, allowing for a patchwork of security measures that malicious actors can exploit [6, 9, 13]. While emerging technologies like HARS and LEO-based PNT offer promising pathways to enhanced resilience, their widespread deployment requires overcoming substantial financial and logistical hurdles, as well as establishing clear policy and international coordination [1, 10, 13]. Without a coordinated, multi-faceted approach addressing these economic, technical, and regulatory barriers, critical infrastructure will remain susceptible to significant disruption from GPS spoofing and jamming.

Limitations and Caveats

This report synthesizes findings from a diverse but limited set of research. Specific cost projections for deploying alternative PNT systems like eLoran across a representative sample of critical infrastructure facilities, including installation and maintenance over 10 years, are not available [3]. The breakdown of the estimated $100 billion annual economic damage by specific sectors (e.g., energy, finance, transportation) is also not provided, which limits the ability to prioritize investment in countermeasures based on

sector-specific impact [1]. Furthermore, while the report identifies emerging technologies like HARS and LEO-based PNT as promising, detailed performance metrics (e.g., detection rate, false positive rate, mitigation time) for currently deployed or piloted systems are scarce [1, 8]. There are also ongoing methodological disagreements regarding the precise cost-benefit analysis of comprehensive solutions versus accepting risk, and how best to model and mitigate cascading risks in complex, interdependent systems [28, 29, 30, 31, 18, 27].

Sources

[1] [gov] Ntia Comments Establishment Interference Temperature Metric - ntia.gov - https://www.ntia.gov/fcc-filing/2004/ntia-comments-establishment-interference-temperature-metric-quantify-and-manage-interference-and

[2] [gov] Doc Study On Economic Benefits Of Gps - space.commerce.gov - https://space.commerce.gov/doc-study-on-economic-benefits-of-gps/

[3] [gov] 1979 DoD AR - history.defense.gov - https://history.defense.gov/Portals/70/Documents/annual_reports/1979_DoD_AR.pdf?ver=2014-06-24-150813-163

[4] [peer-reviewed] Article - sciencedirect.com - https://www.sciencedirect.com/science/article/abs/pii/S0926580520310608

[5] The Trap Closes - dosadinews.net - https://dosadinews.net/the-trap-closes/

[6] 1 Gallardo Lopez Sas Spring 2025 - review.sto.nato.int - https://review.sto.nato.int/images/Papers/1-Gallardo-Lopez-sas-spring-2025.pdf

[7] [preprint] Html - arxiv.org - https://arxiv.org/html/2509.13600v1

[8] Gnssdisruptions - gpsalliance.org - https://www.gpsalliance.org/gnssdisruptions

[9] [peer-reviewed] Articles - pmc.ncbi.nlm.nih.gov - https://pmc.ncbi.nlm.nih.gov/articles/PMC12747701/

[10] [peer-reviewed] 269797648 Analysis Of GNSS Interference Impact On Society An - researchgate.net - https://www.researchgate.net/publication/269797648_Analysis_of_GNSS_Interference_Impact_on_Society_and_Evaluation_of_Spectrum_Protection_Strategies

[11] Paperinformation - scirp.org - https://www.scirp.org/journal/paperinformation?paperid=31514

[12] [peer-reviewed] Articles - pmc.ncbi.nlm.nih.gov - https://pmc.ncbi.nlm.nih.gov/articles/PMC5982992/

[13] [edu] Lo InsideGPS SepOct2009 - web.stanford.edu - https://web.stanford.edu/group/scpnt/gpslab/pubs/papers/Lo_InsideGPS_SepOct2009.pdf

[14] Smart City Executive Brief Infrastructure Protection And Con - iankhan.com - https://iankhan.com/smart-city-executive-brief-infrastructure-protection-and-continuity/

[15] Gnss Security And Cybersecurity What Are The Parallels - safran-navigation-timing.com - https://safran-navigation-timing.com/gnss-security-and-cybersecurity-what-are-the-parallels/

[16] Navigating The Unknown The Risks Of Gnss Outages - starburst.aero - https://starburst.aero/news/navigating-the-unknown-the-risks-of-gnss-outages/

[17] RAND RR2970 - rand.org - https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2970/RAND_RR2970.pdf

[18] [gov] Gps Finalreport618 - nist.gov - https://www.nist.gov/system/files/documents/2020/02/06/gps_finalreport618.pdf

[19] [peer-reviewed] Cyber Security Incidents on Critical Infrastructure and Industrial ... - https://dl.acm.org/doi/10.1145/3057039.3057076

[20] [preprint] Autonomous AI-based Cybersecurity Framework for Critical ... - arXiv - https://arxiv.org/pdf/2507.07416

[21] Country case study: United States: Managing Emerging Critical Risks - https://www.oecd.org/en/publications/managing-emerging-critical-risks_1f9858ea-en/full-report/country-case-study-united-states_9bd860ba.html

[22] Critical Infrastructure Security and Resilience - CISA - https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience

[23] What Is Critical Infrastructure in Cybersecurity? - Gigamon Blog - https://blog.gigamon.com/2026/03/03/what-is-considered-critical-infrastructure-in-cybersecurity-and-why-is-it-important/

[24] [gov] Automation & Vulnerability Management | CSRC - https://csrc.nist.gov/nist-cyber-history/automation-metrics/chapter

[25] [blog] Top 5 Challenges in Implementing Security Requirements (And How ... - https://www.securitycompass.com/blog/top-5-challenges-implementing-security-requirements/

[26] [peer-reviewed] Global navigation satellite systems as critical infrastructure - https://www.sciencedirect.com/science/article/pii/S2590061725001012

[27] Observations of trends in GPS anomalies affecting aviation - Aireon - https://aireon.com/wp-content/uploads/2025/05/Aireon-White-Paper-GPS-Anomaly-Trends.pdf

[28] Why Threat Actors Target Energy and Telecom During Tensions - https://falconfeeds.io/blogs/critical-infrastructure-message-threat-actors-target-energy-telecom-tensions

[29] Positioning, Navigation, and Timing - CISA - https://www.cisa.gov/topics/risk-management/positioning-navigation-and-timing

[30] [peer-reviewed] Development status and challenges of anti-spoofing technology of ... - https://www.frontiersin.org/journals/physics/articles/10.3389/fphy.2024.1425084/full

[31] Impact of Jamming & Spoofing on GNSS Positioning - https://www.unmannedsystemstechnology.com/feature/impact-of-jamming-spoofing-on-gnss-positioning/

[32] [peer-reviewed] Resilience analysis of interdependent critical infrastructure systems ... - https://www.sciencedirect.com/science/article/abs/pii/S1874548221000500

[33] [peer-reviewed] Analysing the risks of failure of interdependent infrastructure networks - https://www.cambridge.org/core/books/future-of-national-infrastructure/analysing-the-risks-of-failure-of-interdependent-infrastructure-networks/8D5E98315FD782AC95DEB6DD0CA19EF6

[34] [gov] 6 CFR Part 29 -- Protected Critical Infrastructure Information - eCFR - https://www.ecfr.gov/current/title-6/chapter-I/part-29

[35] [peer-reviewed] Risk Analysis and Mitigation Strategy of Power System Cascading ... - https://www.mdpi.com/2227-9717/13/1/45

[36] Swiss Re explores cascading effects of natural disasters and other ... - https://www.eqs-news.com/news/corporate/beyond-broken-infrastructure-swiss-re-explores-cascading-effects-of-natural-disasters-and-other-key-emerging-risks/385fc780-4d4f-4ef8-92d8-1a9bb1a06273_en

[37] OSNMA: A step toward multi-layered GNSS security - https://novatel.com/tech-talk/velocity-magazine/velocity-2024/a-step-toward-multi-layered-gnss-security

[38] [gov] RADIO FREQUENCY INTERFERENCE MITIGATION ... - NITRD.gov - https://www.nitrd.gov/nitrdgroups/images/7/76/Radio_Frequency_Interference_Mitigation_for_Planned_SMAP_Radar_and_Radiometer.pdf

[39] [gov] Cost-Benefit Analysis of NOAA Commercial Data Program Radio ... - https://www.space.commerce.gov/wp-content/uploads/2022-01-RO-data-buy-cost-benefit-analysis.pdf

[40] Revealing the Hidden Risks: GNSS Spoofing in Aviation - Spirent - https://www.spirent.com/assets/u/case-study-revealing-the-hidden-risks-gnss-spoofing-in-aviation