Flash | Citi Research

08 Jul 2026 10:35:01 ET | 8 pages

North America Systems Software

What Could SpaceX's Success Mean for the Cyber Complex?

Fatima Boolani[AC]

Mark Zhang

Joel Omino

CITI'S TAKE

SpaceX's ambitions around expanding broadband connectivity via hardware and other physical operational technology (OT) form factors across both civilian and defense networks/domains has got us ruminating on cybersecurity implications. While the external/third-party commercial opportunity for cyber vendors doesn't necessarily feel imminent or immediately obvious, we proffer that the company's success in democratizing access and speed of connectivity has potential to invigorate IoT/IIoT/OT security priorities for its downstream economically-sensitive-skewing customers, as non-traditional connected-device volumes look poised to expand, and with it compound pre-existing supply chain risks (IT-to-OT, OT-to-IT). Alongside open-source and commercial LLMs showcasing ever-increasing proficiency in identifying staggering volumes of novel/previously-undiscovered exploitable vulnerabilities (particularly pernicious in a geopolitical context), we make the case that OT cyber focus (itself a relatively under-invested niche) could enjoy renewed importance and which should benefit independent, "assurance-layer" vendors.

More non-traditional connected devices = more diffuse/arcane attack surface to defend: In the OT context, we see SpaceX's success as a potential catalyst for more meaningful volume growth in non-traditional connected devices (think more SCADA-based, industrial control systems or ICS) for downstream customers in critical-infrastructure-skewing economic sectors (airlines, maritime/shipping operators). This ultimately would imply a widening of the aggregate scope and "attack surface area" of these connected and increasingly-physically-diffuse environments. OT/ICS security has generally been a more niche and relatively under-invested-in domain compared to "classic IT," carrying fundamentally different protocols (and requisite tech stack, skills) for defensive hygiene. And with AI too infusing this arena (AI labs/frontier models unearthing higher volumes and novel flavors of vulnerabilities, especially unique in OT OS and software stacks), we'd anticipate fleet-level anomaly detection, hardware attestation, and firmware integrity monitoring demands, alongside conventional OT access control/segmentation/monitoring imperatives likely seeing elevated (albeit steadily) importance.

Who could win: We think success is likely to manifest in private companies with subject-matter expertise in the traditional ICS security domain (Claroty, Dragos), but would also highlight FTNT, and to a lesser extent PANW's OT efforts here, along with select forays from Armis (now part of NOW).

See Appendix A-1 for Analyst Certification, Important Disclosures and Research Analyst Affiliati

