ORION FORUM

The Contested LEO Battlespace: The Fight for Connectivity, Control, and Decision Advantage

SEPTEMBER 1, 2026

The war in Ukraine is exposing a fundamental change in modern conflict. Low Earth orbit (LEO) constellations are no longer simply a supporting layer that provides communications, imagery, navigation, and data to forces fighting below. It is becoming part of the battlespace itself, not necessarily because satellites are being destroyed in orbit, but because military forces are increasingly fighting over access to the services those satellites provide. Russia's improving ability to interfere with Starlink, its exploitation of commercial satellite communications, Ukraine's subsequent use of network controls to deny that access, Moscow's broader counterspace activity, and Russia's development of its Rassvet LEO constellation point toward a new operational reality. The central question for future forces will not be whether they can connect to space, but whether they can preserve decision-quality connectivity when access to space is deliberately contested. This question often arises because of the growing reliance on satellite technology for military and private-sector use.

The distinction between contested space and contested access to space is important. The most consequential space fight over Ukraine is not currently a campaign to destroy satellites. It is a struggle over terminals, uplinks, navigation signals, software permissions, ground infrastructure, electromagnetic access, cyber vulnerabilities, and the movement of information between sensors, commanders, and weapons. A constellation may remain intact while the military capability depending on it becomes degraded at a critical moment. Orbital resilience alone is therefore insufficient because the operational requirement is not simply keeping satellites alive. It is preserving the mission functions those satellites enable. Starlink demonstrated the importance of this distinction early in the war. Russia attacked or disrupted

significant portions of Ukraine's conventional communications infrastructure, while Starlink provided a distributed alternative that was difficult to eliminate through conventional means. The network became important to command and control, intelligence sharing, drone operations, logistics, and coordination across dispersed formations. Its proliferated architecture offered substantial resilience because thousands of satellites, changing orbital geometry, mobile terminals, and distributed networking made the service difficult to disable as a whole.

Russia's response provides one of the war's most important adaptation stories. Moscow first sought to disrupt Starlink, then Russian forces increasingly exploited Starlink terminals themselves, including on unmanned systems. Ukraine and SpaceX responded in February 2026 with a verification process intended to allow authorized Ukrainian terminals to operate while blocking unauthorized Russian terminals. Russia subsequently intensified electronic warfare against Starlink-enabled Ukrainian operations while accelerating work on a sovereign LEO alternative. This progression from disruption to exploitation to software-based denial to renewed electronic attack and indigenous capability development shows how quickly a technological advantage can become an operational competition. Russia's improving jamming capability illustrates how that competition is moving toward the tactical edge. Reuters reported in July 2026 that Russian forces were deploying electronic warfare systems intended to disrupt Starlink connectivity used by Ukrainian mid-range drones attacking logistics, fuel storage, air defense installations, and command centers behind Russian lines. Ukrainian forces were already targeting some of those systems to restore freedom of operation. The significance is not that Russia has defeated Starlink across Ukraine, because it has not. The important development is Russia's ability to create localized areas where a highly resilient global network becomes less dependable at the place and time Ukrainian forces need it. This exposes a vulnerability military planners should not overlook. A proliferated constellation may be extraordinarily difficult to destroy or disable globally, but a tactical user must still establish and maintain a usable connection. Russia does not need to attack thousands of satellites to produce a battlefield effect. It can interfere with the user link, disrupt navigation, attack supporting infrastructure, complicate terminal operations, or force the operator onto a less capable alternative. The vulnerable seam is increasingly the path between the tactical user and the service rather than the satellite itself, and Ukraine is taking notes as Russia's

constellation gets closer to reality. It will be the first time that a dedicated effort against space assets will present itself in modern conflict. This changes the operational meaning of satellite resilience. If a drone loses communications during a critical targeting sequence, the health of the constellation provides little immediate value. If a headquarters loses reliable connectivity during a command transition, global network availability does not solve the local problem. Commanders must therefore begin thinking about satellite access as they already think about electronic warfare threat areas, communications dead zones, or air defense coverage. Connectivity must be understood geographically and temporally, protected where necessary, restored when disrupted, and supported by alternatives when restoration is impossible. This is the tactical action that supports survivability, the most important aspect of warfare.

The Ukrainian response reinforces this point because electronic warfare systems interfering with satellite connectivity become high-value targets themselves. When suppressing a jammer restores the communications pathway required for subsequent drone operations, access to LEO becomes directly connected to targeting and fires. The result resembles a communications equivalent of suppression of enemy air defenses, in which freedom to exploit one capability depends upon reducing the adversary's ability to deny it. Space-enabled communications are consequently becoming inseparable from operations in the electromagnetic spectrum.

Russia's Volna Kupol Garant provides a tangible example of how this contest is developing. According to Ukrainian Defense Ministry adviser Serhii Beskrestnov, the Russian electronic warfare system is designed to interfere with Starlink by transmitting powerful interference from the ground toward passing satellites in the 14 to 14.5 GHz uplink band. The system is reportedly distributed across six trailers, can operate from generators or external power, and can affect Starlink connectivity across an area of up to approximately 20 square kilometers. Rather than attempting to disable the constellation itself, Volna Kupol Garant creates a localized area in which Ukrainian forces may lose reliable access to the service. Reuters subsequently reported that Ukrainian forces had detected approximately ten such systems and were deliberately targeting them, with one Ukrainian drone commander reporting that Starlink-equipped aircraft resumed operating normally after one installation was struck. The Russian counter-LEO effort may also be broader than the Volna Kupol Garant alone. On August 25,

2026, the General Staff of the Armed Forces of Ukraine reported that Ukrainian forces had struck a specialized **Peresvet-M electronic warfare complex in Luhansk** and, separately, a **Starlink satellite-communications jamming station in Myrnyi, occupied Crimea**. The General Staff's identification of the two as separate targets is noteworthy because it suggests that Russia may be fielding multiple electronic warfare capabilities relevant to the contest over satellite-enabled operations. Publicly available information does not yet establish the precise capabilities, physical dimensions, operating frequencies, or relationship of Peresvet-M to Volna Kupol Garant, so it would be premature to characterize Peresvet-M as a larger or more capable Starlink jammer. What the August strikes do demonstrate is that specialized electronic warfare and satellite-communications denial systems are becoming important enough to be deliberately identified, located, and attacked as part of Ukraine's strike campaign.

The contest also extends beyond electronic warfare into commercial network control. Ukraine's Starlink verification process demonstrated that battlefield access could be denied through authentication rather than jamming. Network identity, geolocation, software configuration, service permissions, and provider policy can therefore produce operational effects without physically attacking either the terminal or satellite. This introduces a new dependency because a commercial network may be technically capable of supporting a mission while software settings, geographic restrictions, or provider policies affect how it can be employed. The control plane of the network is becoming another form of operational terrain. Russia's most consequential long-term response may therefore be its effort to remove that dependency. Bureau 1440 began deploying production satellites for its Rassvet broadband constellation in 2026 as part of Russia's attempt to establish sovereign LEO connectivity. The system remains far smaller and less mature than Starlink, and Russia faces substantial manufacturing, launch, terminal, and networking challenges. However, Rassvet does not need to match Starlink to matter militarily. Even a smaller constellation could provide useful connectivity for selected missions, geographic areas, mobile command posts, unmanned platforms, reconnaissance systems, and other users requiring beyond-line-of-sight communications. The rationale becomes clear when viewed through Russia's experience in Ukraine. Moscow observed the military value of distributed LEO communications, used the same commercial architecture where possible, and then experienced the vulnerability of depending on a provider it did not

control. A sovereign constellation reduces that dependency while creating new military options. Rassvet is therefore important not because it currently equals Starlink, but because it represents Russia's attempt to ensure that future access to LEO communications cannot be denied through a foreign company's authentication system.

If Rassvet matures, the battlefield could move toward a more symmetrical competition in which both sides employ distributed satellite-enabled networks while attempting to degrade the other's access. The contested LEO battlespace would then involve far more than competing satellites overhead. It would combine orbital systems, terrestrial infrastructure, electronic warfare, cyber operations, commercial networks, terminals, and operational decision-making into a single contested architecture. Russia's broader counterspace behavior suggests that this competition will extend beyond communications. Moscow continues to develop electronic attack, cyber, orbital, and other counterspace capabilities, while Russian military satellites have demonstrated maneuvering that has drawn scrutiny when conducted near Western commercial spacecraft. Commercial imagery and communications supporting Ukraine have become operationally important because they provide capabilities once available primarily through national military systems. As commercial services contribute more directly to reconnaissance, targeting, communications, and planning, the distinction between civilian infrastructure and military support becomes increasingly difficult to maintain. **Destructive attacks against satellites remain only one counterspace option and may often be less attractive than reversible or localized effects**. Physical destruction creates escalation risks, political consequences, and potentially dangerous orbital debris, while jamming, spoofing, cyberattacks, service denial, and interference can produce useful military effects without destroying spacecraft. Selective denial may therefore become a defining characteristic of the contested LEO environment because an adversary does not require permanent destruction when temporary disruption at the right moment can break a kill chain.

Cyber operations expand the attack surface further because the satellite is only one component of the system. Ground stations, terminals, user accounts, software, cloud infrastructure, authentication mechanisms, terrestrial backhaul, and network management all contribute to delivering the service. The cyberattack against Viasat at the beginning of

Russia's 2022 invasion demonstrated that a satellite communications capability could be disrupted by attacking the network surrounding the spacecraft rather than the spacecraft itself. The modern space fight consequently extends from orbit through the ground segment to the tactical user. Position, navigation, and timing (PNT) add another dimension because connectivity alone does not guarantee mission effectiveness. Russian GPS interference has repeatedly complicated Ukrainian unmanned and precision operations. A drone may retain communications while losing confidence in its navigation solution, or it may retain navigation while losing the communications path required for human control or updated targeting. Although these functions rely on different technical systems, they converge within the mission, meaning that resilient operations require understanding the health of the entire information architecture rather than any single network.

This pressure helps explain the growth of autonomous navigation, inertial systems, machine vision, preprogrammed routes, and fiber-optic control. These technologies respond to an environment in which neither continuous RF connectivity nor satellite navigation can be assumed. They do not diminish the importance of LEO. Instead, they demonstrate why future forces will need multiple ways to communicate, navigate, sense, and complete the mission when individual pathways become unavailable. Reinforcing redundancy in every aspect of combat operations. The resulting architecture must be hybrid rather than dependent on any single satellite service. Satellite communications, tactical radios, mesh networks, terrestrial systems, airborne relays, alternative navigation, and autonomous fallback modes must complement one another. The ability to transition rapidly among those pathways will become more important than maximizing the performance of one network. The answer to Russian Starlink jamming therefore cannot simply be better Starlink, just as the answer to Rassvet cannot be one capability designed to neutralize Rassvet. Both approaches would preserve the structural vulnerability created by dependence on a single solution.

A more durable architecture must be designed from the beginning to operate through disruption, but technology alone will not create resilience. Commanders need to know which networks remain available, where interference is occurring, whether navigation data can be trusted, what cyber anomalies are emerging, and which alternatives can still support the

mission. If those conditions remain distributed across technical systems and organizational stovepipes, a force can possess enormous communications capacity while lacking the understanding necessary to employ it under pressure. The contested LEO battlespace is therefore as much a common operating picture and command problem as it is a satellite problem. This is where the competition becomes one of Decision Advantage. The force that prevails will not necessarily possess the largest constellation, strongest jammer, or most sophisticated terminal. It will be the force that detects degradation sooner, understands the operational consequences faster, identifies which alternative remains viable, possesses the authority to transition, and continues executing before the adversary can exploit the disruption. Connectivity has military value only when it preserves the ability to understand, decide, and act.

Ukraine has provided the early outline of this future. Starlink created a communications advantage; Russia adapted by attempting to disrupt the service and then exploiting it for its own operations; Ukraine and SpaceX responded through software-based authorization, and Russia increased localized electronic warfare while developing an independent LEO constellation. At the same time, cyber operations, navigation warfare, autonomous systems, fiber-optic control, commercial imagery, and counterspace activity have expanded the competition beyond any single network. What began as an extraordinary example of commercial satellite communications supporting a nation at war is becoming evidence of a much larger transformation. The contested LEO battlespace is therefore not fundamentally a contest over who owns the most satellites. It is a contest over whether a force can preserve command, sensing, navigation, targeting, and decision-making when the space-enabled architecture supporting those functions is under sustained attack. Russia’s advances against Starlink matter because they demonstrate that even a proliferated and resilient constellation can be challenged at its operational seams, while Rassvet matters because it shows that adversaries are building their own alternatives after learning from Starlink’s battlefield impact. Future forces must consequently design for contested access rather than assume continuous connectivity. The military that succeeds will not be the one whose network never fails, because that expectation is increasingly unrealistic. It will be the one that preserves enough understanding, authority, connectivity, and options to continue deciding and acting when

portions of the network inevitably do.

Disclaimer: *Orion Policy Institute (OPI) is an independent, non-profit, tax-exempt think tank focusing on a broad range of issues at the local, national, and global levels. OPI does not take institutional policy positions. Accordingly, all views, positions, and conclusions represented herein should be understood to be solely those of the author(s) and do not necessarily reflect the views of OPI.*

Author's Short Bio

Bill Edwards is a retired U.S. Army Colonel with more than 35 years of experience in operational and technical security, counterterrorism, counterintelligence, surveillance and counter-surveillance, and emergency preparedness across government and private-sector environments. After retiring from military service in 2018, Bill founded Phoenix 6 Consulting, a customized security services firm focused on risk-informed security design, emerging threat mitigation, and operational resilience. He currently serves as a Director of C-UAS Operations and Training at ENSCO.

He previously served as Principal, leading Thornton Tomasetti's Security Consulting Group from 2018 to 2022. More recently, Bill served as President, Federal and Public Safety for Building Intelligence, where he led federal engagement and market adoption of trusted access management software. During his military career, Bill served as Director of Intelligence for Theater Special Operations Command–North (USSOCOM), a role requiring close coordination across the U.S. Department of Defense, federal law enforcement, and interagency partners. In this capacity, he designed and implemented a cohesive counterterrorism information-sharing architecture—known as the "Blue Network"—integrating domestic and international partners to support U.S. homeland security and defense missions.

Bill deployed multiple times to Iraq, operating and commanding large bases in Al Anbar, Dhi Qar, and Basra Provinces, where he was responsible for operations, force protection, and infrastructure security. His work included the planning, design, and execution of layered security systems to counter evolving threats in complex operational environments. An accomplished author and educator, Bill co-authored Inside Abu Ghraib: Memoirs of Two U.S. Military Intelligence Officers, which examines leadership under extreme adversity and the

impact of deployments on military families. He has published more than 134 articles on security-related topics, with a particular focus on the evolution of small unmanned aircraft systems (sUAS) and their implications for public safety
and societal security. He teaches leadership, strategic communications, and negotiations to senior Air Force officers at the Air Force War College and instructs students at The Citadel, Columbia Southern, and Towson Universities on the operational and security impacts of drone technology.

Bill is widely recognized as a transformational leader with a proven ability to build and motivate teams, align diverse stakeholders, and deliver results in high-risk, high-consequence environments. His private-sector experience spans critical infrastructure, professional sports, transportation, commercial real estate, healthcare, cultural and religious institutions, and city, county, state, and federal government projects. Bill holds ASIS International board certifications as a Certified Protection Professional (CPP), Physical Security Professional (PSP), Certified Counter UAS Security Professional (CCUSP), and Professional Certified Investigator (PCI). He is a FEMA Level I Continuity Planner, a licensed FAA Part 107 Remote Pilot, and the developer of sUAS training courses currently offered through ENSCO.