



THE PRIVATIZED KILL CHAIN: WHO CONTROLS MILITARY C2?

Ukraine, Commercial Satellite Communications and the Sovereignty Risks of Private Space Infrastructure

An assessment of how military reliance on commercial space and digital infrastructure creates operational advantages, external dependencies and new command-and-control vulnerabilities. Using Ukraine as the principal operational case, it examines how access, service policy and technical control affect military C2, ISR and UAV operations—and the resilience of NATO forces.

DATE

15 October 2026

GEOGRAPHIC AREA

Ukraine / NATO

INTELLIGENCE DOMAIN

Space / C4ISR / Military Communications

AUTHOR

Cyber & Space Security Team

STATUS

For Editorial Approval

Executive Assessment

Commercial access expands capacity and recovery options, but availability is not sovereign assurance.

Commercial space and digital services have altered the cost and speed of military connectivity. In Ukraine, commercial satellite communications, imagery and cloud-enabled data tools have helped restore links when terrestrial infrastructure was damaged, support dispersed command posts and move information between sensors, staffs and units. Their value lies in scale, rapid fielding and distributed architecture. They do not, by themselves, provide command authority, secure integration or a complete sensor-to-shooter chain.

The operational advantage creates an external dependency. A military user may own a terminal while a provider controls network access, software configuration, service geography, prioritisation and technical support. A government may have legal authority over some services or contracts without controlling the company's entire infrastructure. Access can therefore change through policy, regulation, cyber attack, congestion, licensing or a provider decision faster than a sovereign military system can be replaced.

The distinction is between technical resilience and sovereign control. A constellation may be physically distributed and difficult to disable, yet a terminal's authentication, software, gateway access or service policy may remain centrally managed. Commercial capacity can make a military network more resilient against physical attrition while leaving it exposed to a different failure class: a change in access conditions outside the operational chain of command.

Reporting on 14 October 2026 provides a current, but not yet independently verified, illustration. Reuters and the Associated Press reported Ukrainian claims that speed or usage restrictions affecting military-grade satellite terminals disrupted some drone missions. Reuters described Ukrainian accounts of disconnections above stated speed thresholds; AP reported that connections later improved but remained inadequate for some missions. Reuters also reported differing descriptions of Starlink and Starshield, while SpaceX's chief executive attributed limits on military services to the US government. Public technical logs and an independent assessment of the affected service were not available in those reports. The incident should be treated as a reported operational disruption, not proof of motive or a complete account of technical responsibility.

The central judgment is that commercial infrastructure should be treated as an operational dependency with a defined assurance level, not as guaranteed sovereign capacity. It is an effective source of scale and resilience when commanders have alternatives, pre-agreed wartime access, compatible terminals and the authority to shift traffic. It becomes mission-critical when operational processes are designed around one provider without a tested fallback. The evidence supports a model of layered dependence, not the claim that one company controls an entire military kill chain.

Commercial Infrastructure as a Military Enabler

Different commercial services perform distinct functions across communications, collection and data handling.

Commercial SATCOM provides reach when fibre, cellular networks and terrestrial microwave links are damaged, congested or unavailable. Low Earth orbit systems can deliver low-latency broadband to small terminals and can be deployed without waiting for a national fixed network. This combination is particularly useful for mobile units, dispersed headquarters and temporary sites. It can also increase the number of network entry points, complicating an adversary's effort to suppress all communications through attacks on a small set of fixed nodes.

Commercial earth-observation imagery contributes a different function. It can broaden collection, increase revisit opportunities and provide imagery to governments, analysts and, in some cases, operational users. The information still requires tasking, processing, geolocation, fusion with other intelligence and dissemination to the right echelon. Cloud-hosted tools and mapping services can shorten those steps, but they introduce dependencies on identity management, data residency, APIs, software updates, network availability and contractual access.

These systems are not interchangeable. SATCOM moves data; imagery supplies observations; cloud platforms store or process information; mapping services provide geospatial context. Each can be supplied by different organisations and may operate under different legal and technical arrangements. A single command workflow may depend on several providers even where the end user experiences one application.

Commercial systems are generally designed for large customer bases and rapid updates. That can make capacity more affordable and adaptable than bespoke military procurement. It can also mean that product roadmaps, maintenance windows, service tiers and security controls are optimised for the provider's broader market. Military users must identify which service features are contractually guaranteed, which are best-effort, and which depend on government intervention during a crisis.

01 — COMMERCIAL SATCOM



FIG. 1 | Ukrainian service member installing a Starlink terminal.

Source: Ukrainian Support Forces Command / Wikimedia Commons.



FIG. 2 | Starlink ground terminal installed outdoors.

Source: Wikimedia Commons (Starlink antenna on the ground).

The Ukraine Operational Case

Ukraine demonstrates operational utility alongside the limits of publicly verifiable evidence.

Ukraine's experience shows the operational value of commercial access under severe infrastructure pressure. Satellite terminals have been used alongside terrestrial networks to restore connectivity at command locations and support military communications. Commercial satellite imagery and open data also helped external governments and analysts observe force movements before and during the invasion. These functions enabled continuity and wider situational awareness; public reporting does not establish that commercial systems alone carried Ukraine's command network or supplied a complete real-time targeting chain.

The cyber attack on the Viasat-operated KA-SAT network on 24 February 2022 demonstrates both the military relevance and the limits of broad claims. The European Union formally attributed the operation to Russia and stated that it caused outages in Ukraine and several EU member states. Viasat's incident account described destructive commands against modems in a consumer-oriented network partition and said directly managed mobility and government users on KA-SAT were not affected. The event therefore supports the assessment that commercial satellite service partitions and ground management systems can have cross-border consequences; it does not show that all satellite communications or military users were disabled.

Commercial connectivity also gained institutional importance. In June 2023, the US Department of Defense confirmed that it had contracted for Starlink services for Ukraine, formalising a government role in sustaining a capability that had initially expanded through private and donated support. In February 2026, Starlink's public service notice said that terminals operating in Ukraine required approval on a government whitelist, coordinated with Ukrainian ministries. This illustrates that service availability can be conditioned by both provider systems and state authorization.

The reported 14 October 2026 restriction affecting high-speed drone terminals should be assessed against this history, but with caution. Reuters and AP reported Ukrainian officials' accounts of disrupted missions and later partial improvement. The reports differ in how they describe the affected service and the relationship between Starlink and Starshield. That distinction matters because commercial Starlink and government-oriented Starshield have different ownership and control arrangements, even where they draw on related infrastructure. Until the parties publish technical details, the defensible conclusion is narrower: a change in service behaviour was reported to affect some Ukrainian drone operations, and commanders apparently lacked advance notice sufficient to prevent disruption.

The case demonstrates how rapid adoption can precede the development of mature governance. Wartime users gain speed and coverage first; terminal management, service assurance, alternative providers, classification, cyber security and command procedures may develop later. The operational question is not whether the system was useful. It is whether critical units could continue their assigned tasks when access was degraded, restricted or uncertain.

The External-Control Problem

Ownership, technical control, legal authority and operational dependence do not necessarily align.

Four forms of control should be separated. Physical ownership concerns satellites, gateways, terminals and data centres. Technical control includes network management, authentication, software configuration, geofencing, traffic prioritisation and service restoration. Legal authority covers national regulation, licensing, export controls, contractual obligations and government direction. Operational dependence describes how much a force's actual command process relies on a service. These forms can sit with different actors and jurisdictions.

A military may possess equipment but lack authority to alter the network's software or coverage policy. A government may regulate or contract for a service but lack direct control over global infrastructure or the provider's commercial decisions outside the contract. An allied government may pay for service without having authority to direct a provider's technical operations. The result is a split-control arrangement in which military commanders receive the operational consequence but may not control the mechanism that produces it.

Contract language can reduce uncertainty but cannot eliminate all risk. Service-level commitments, priority access, incident notification, continuity clauses, data-handling requirements, government access rights and wartime coordination arrangements can clarify responsibilities. Their value depends on enforceability across jurisdictions, the technical ability to implement them and whether the provider can meet them during simultaneous demand or attack.

Policy change is only one failure path. Network congestion, software release errors, cyber intrusion, gateway damage, sanctions, export restrictions, spectrum interference or a provider insolvency could also interrupt service. A military dependency becomes strategically

significant when a commercial change affects mission execution before an alternative can be activated. The practical exposure is therefore a function of switching time, not merely the probability that a provider will withdraw.

Operational dependence becomes acute when the time needed to obtain a provider or government decision exceeds the time available to reconfigure a mission. Notification clauses, priority arrangements and escalation contacts can reduce uncertainty, but their value depends on tested procedures and clear authority across national jurisdictions. A commander should know which changes can be handled locally, which require national intervention and which cannot be reversed during the operation. Public information rarely reveals these service-level details, so open-source assessment can identify the dependency but cannot certify a particular contract's assurance level.

C2 and Kill-Chain Dependency

Commercial services may enable individual links without carrying the entire kill chain.

The functional chain is sensor, communications, data fusion, command decision, targeting, weapon or UAV control, and battle-damage assessment. Commercial systems may support one or several links, but no single commercial network should be assumed to carry the entire chain. A sensor may use one provider to transmit imagery, a government network to move classified data, and a separate tactical radio for command. The interfaces and handoffs between them are as consequential as the underlying services.

Commercial connectivity is enabling when it improves reach or throughput but the unit can continue by other means. It becomes substitutable when a trained and tested alternative can assume the mission within an acceptable time. It is mission-critical when its loss forces a unit to stop, delay or materially reduce an assigned task. A single point of failure exists only where a specific function lacks a workable path around the failed component; provider count alone does not establish redundancy if all providers share gateways, cloud identity, power, fibre routes or software.

Connectivity is not equivalent to command. A high-bandwidth link can carry video and sensor data, but command authority remains with military institutions, and the quality of decisions depends on validation, procedures, trained staff and the ability to operate under degraded conditions. The chain can fail through latency, stale data, unclear authority, poor interoperability or a target that has moved, even where the network is available.

Commercial access restrictions can alter this chain unevenly. A geographic limit may affect terminals in a specific area; a speed limit may affect moving platforms while leaving fixed headquarters online; prioritisation may preserve government traffic but reduce other users' capacity. Such controls can change which missions are feasible without producing a complete outage. Operational plans should therefore define degraded modes by mission and echelon rather than use a binary connected/disconnected assumption.

For planning purposes, each link should be classified as enabling, substitutable or mission-critical for the specific task. A commercial service is enabling when its loss reduces speed or convenience but leaves the unit able to complete the mission. It is substitutable when another path can carry the required data within an acceptable delay. It is mission-critical when the loss prevents a necessary command, targeting or control function before a fallback can be activated. These classifications may differ between units using the same provider and should be verified through no-service exercises rather than inferred from system ownership.

02 — UAV DIGITAL TARGETING



FIG. 3 | Ukrainian military vehicles carrying UAV-related equipment.

Source: 45th Artillery Brigade / Wikimedia Commons.



FIG. 4 | Ukrainian operator preparing UAV equipment.

Source: 148th Artillery Brigade / Wikimedia Commons.

Resilience and Failure Modes

Distributed infrastructure reduces some physical risks while leaving policy and network dependencies.

Failure modes include jamming or interference, cyber compromise, terminal loss, satellite or gateway disruption, congestion, power loss, software change, authentication failure, geofencing, provider outage, legal restriction and supply-chain interruption. Their effects differ by scale. A local terminal loss may be managed by moving traffic to another device. Regional gateway disruption may force rerouting and reduce throughput. A policy or identity-system failure could affect many users at once.

The KA-SAT incident shows that an attack on ground-based network management can produce effects beyond the intended user group. It also shows why system segmentation and recovery procedures matter. Viasat reported that the attack targeted a consumer-oriented partition and did not affect its directly managed government or mobility customers on the same satellite. This distinction cautions against treating a satellite, a service and its user networks as a single object.

Electronic attack against user links can be local and intermittent; cyber effects may propagate through shared management systems; commercial congestion may be predictable during high demand; a provider policy change may be abrupt but geographically or functionally bounded. Military response differs across these cases. Radio discipline and alternate bearers may mitigate local jamming, while cyber

incidents require isolation and restoration. Contractual and political channels may address service policy, but they do not restore lost connectivity immediately.

Resilience is not simply the number of satellites in orbit. It includes terminals that can connect to different systems, gateway diversity, power and backhaul protection, encryption, key management, trained operators, traffic prioritisation, rapid reconfiguration and the ability to fight through loss of cloud or network services. A distributed constellation improves survivability against some physical attacks; it does not automatically guarantee continuity of a user account or application.

The distinction between local and systemic denial is consequential. A damaged terminal or blocked user account may constrain one team; a gateway failure, common software defect, regional spectrum effect or provider-wide policy change may affect many users at once. Indicators include the geographic spread of service loss, whether unaffected terminals can authenticate, whether alternate gateways remain available and whether other providers show correlated degradation. These indicators help distinguish an isolated fault from a common-mode failure. Public reporting may not disclose enough technical detail to identify the initiating cause, so operational response should not depend on early attribution.

Commercial ISR and Targeting

Commercial imagery can widen collection, but tasking, fusion and dissemination remain decisive.

Commercial imagery expands access to observation and can help track fixed infrastructure, force concentrations and changes over time. Its utility depends on revisit interval, resolution, weather, collection priority, processing latency, geolocation accuracy and the time required to reach an operational user. The nominal availability of imagery is not the same as a timely, validated target-quality product.

Commercial providers may offer tasking and analytics, but their capacity is finite and customers compete for it. During a crisis, priorities can shift, legal restrictions can affect dissemination, and sensitive sources or methods may require protected government channels. Military ISR remains necessary to fill gaps in coverage, verify changes, detect mobile activity and support classified fusion.

Targeting requires more than an image. Analysts must establish that an object is correctly identified, that the information is current, and that the target remains valid when the weapon is assigned. Deception, camouflage, decoys, movement, cloud cover and deliberate data manipulation can reduce utility. Commercial imagery can cue collection and improve context; it should not be represented as a complete targeting solution.

Dependence can occur in the dissemination layer as much as in collection. If imagery is fused in a commercial cloud platform or accessed through a proprietary application, a change in identity management, API availability or subscription status may delay distribution even when the satellite has collected the data. The assurance test must follow the product from collection to the intended military user.

The usable value of imagery is determined by the full exploitation chain: collection opportunity, tasking priority, downlink, processing, analyst validation, fusion and delivery to the unit. A high revisit rate does not guarantee that the relevant location is observed at the required time, and rapid dissemination does not remove the need to check geolocation, context and source reliability. Deception, concealment and activity between collections can create misleading or incomplete pictures. Commanders should treat commercial imagery as an additional source whose confidence and timeliness are assessed alongside military sensors and reporting from forces in contact.

03 — SPACE BASED ISR



FIG. 5 | Synthetic aperture radar image of Kyiv.

Source: Capella Space / Wikimedia Commons, 29 Nov 2024.

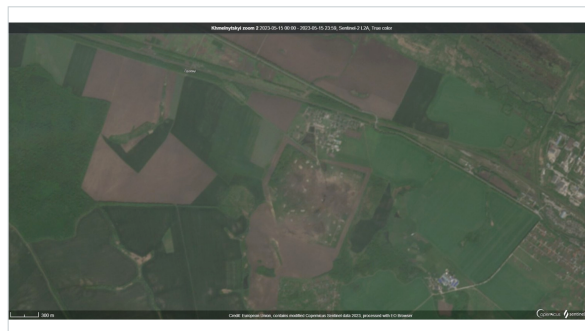


FIG. 6 | Sentinel-2 view of the Khmelnytskyi area.

Source: EU Copernicus Sentinel data, 15 May 2023; EO Browser.

UAV Operations and Connectivity

Network access can support selected mission phases; effects vary by platform and link architecture.

Commercial networks can support command links, mission upload, telemetry, video transmission, coordination and beyond-line-of-sight control. The effect varies by aircraft, mission profile and architecture. A terminal may provide a high-capacity backhaul to a command post rather than a direct control link. A platform may use a commercial network for some phases and radio, inertial navigation or autonomous functions for others.

Public reporting on 14 October 2026 described Ukrainian claims that restrictions on satellite terminals affected some attack and interceptor-drone missions, with reported effects linked to platform speed. This is a reported case, not a general technical rule. Reuters and AP described different details and service labels, and public telemetry was not available. The assessment should not infer that every drone depended on Starlink or that all missions were disabled.

Connectivity can increase the distance between operators and platforms and allow rapid exchange of imagery or mission data. It can also create predictable dependencies on a provider's coverage, network management and approved use. Autonomous functions may reduce the need for a continuous link in some phases, but they do not remove requirements for mission planning, updates, coordination, legal control and post-mission assessment. Claims of autonomous capability should be separated from observed practice.

Units need clear transition procedures for loss of link: which tasks continue, which are suspended, what data is cached locally, how authority is transferred and how operators verify that the platform remains within approved bounds. The purpose is to preserve safe, lawful and controlled operations under degraded connectivity, not to assume that the network will remain continuously available.

A network outage can have different consequences depending on whether the commercial path carries flight control, mission updates, sensor video or only backhaul to a command post. Local autonomy may preserve a preplanned task after link loss, but it does not establish that the mission remains safe, authorized or tactically useful. The unit must know what the aircraft will do on loss of link, what information remains on board and how an operator can terminate or recover the mission. Such behaviours are platform-specific; no general claim about autonomous operation can be drawn from the presence of a satellite terminal.

Sovereignty and Command Authority

The assurance test is whether commanders can preserve access or transition under crisis conditions.

The sovereignty issue is not whether commercial support is useful; it is whether military commanders can guarantee access during a crisis. A state may authorize terminals, pay for service and establish contractual priority while still depending on a provider's technical configuration or the national authorities that regulate it. When the provider is based abroad, escalation, sanctions, export controls and diplomatic relations may affect continuity.

Command authority remains a military responsibility. A provider may control the service but does not thereby assume command of the unit using it. The risk arises when operational plans depend on a service whose access conditions can be changed by actors outside the military chain of command, without adequate notice or a feasible fallback. This is a control and assurance problem, not a claim that private firms direct battlefield decisions.

Alliances add another layer. A member state may contract for access used by a partner, while the service is governed by another state's law and delivered through multinational infrastructure. NATO interoperability therefore requires agreed standards for identity, encryption, data classification, priority access, incident reporting and transition between providers. The alliance must also understand which commercial services are national contributions and which are available under collective arrangements.

Legal authority and wartime continuity should be planned before crisis. Governments can use procurement, licensing and regulation to establish requirements, but safeguards must account for competing civilian demand, cross-border operations and the provider's physical capacity. A contract that promises priority cannot create satellites, gateways or spectrum where none are available.

04 — OPERATIONAL DEPENDENCIES



FIG. 7 | Pole-mounted commercial Starlink terminal.
Source: Wikideas1 / Wikimedia Commons.



FIG. 8 | Ukrainian Sting interceptor UAV and operator.
Source: Ukrainian Armed Forces / Wikimedia Commons.

Mitigation and Military Alternatives

Resilience depends on tested, interoperable alternatives and realistic degraded-mode procedures.

The strongest mitigation is a layered architecture with tested alternatives. Sovereign military SATCOM offers a degree of command assurance and protected services, but costs, acquisition timelines, capacity and terminal availability limit how quickly it can replace commercial broadband. Allied systems can expand capacity, yet access depends on interoperability, national release rules and competing operational demand.

Multi-provider architectures reduce dependence only when they are technically and operationally diverse. Terminals must be able to connect to alternative constellations, gateways and bands; user equipment must be procured in sufficient numbers; network selection and encryption must work across systems; and operators must train to switch under time pressure. Two providers using the same cloud identity, ground station region or supply chain may share a common failure.

Terrestrial radio, fibre, microwave links, tactical relays and mesh networks remain important. They can provide local control and reduce reliance on space-based backhaul, but line of sight, terrain, range, infrastructure damage, electromagnetic signature and bandwidth constrain their use. A resilient force needs methods that can be combined rather than a single substitute expected to reproduce the reach and capacity of a commercial LEO network.

Pre-negotiated wartime contracts, government priority arrangements and notification obligations can reduce uncertainty. They should specify which services are guaranteed, which missions are excluded, who can change access conditions, how incidents are reported and what transition support is available. Such arrangements must be tested in exercises; an untested clause is not an operational fallback.

At unit level, local buffering, alternate communications plans, data minimisation, offline map and mission data, disciplined traffic prioritisation and clear degraded-mode procedures can preserve essential functions during interruption. These measures do not replace secure networks. They reduce the chance that loss of a commercial service immediately removes command options.

Redundancy should be measured by usable mission pathways, not by the count of providers. A second service may offer little resilience if it relies on the same terminals, gateway region, cloud identity, power supply or upstream network. Conversely, a lower-bandwidth radio path can preserve essential command even when it cannot carry video or bulk data. Procurement should match each route to its intended function, define minimum data and latency requirements, and test transitions with the people and equipment expected to operate them. The resulting architecture will cost more than reliance on one commercial service, but it limits the chance that a single decision or technical fault removes every option.

Implications for NATO

Allied integration requires clarity on access, control, interoperability and continuity obligations.

NATO should treat commercial space as both an operational enabler and a dependency requiring assurance. The US Space Force's 2024 Commercial Space Strategy frames commercial integration around operational utility, feasibility, resilience by design and speed to field. The Government Accountability Office's 2025 review describes the Department of Defense's move toward an integrated SATCOM enterprise combining military and commercial options; it also identifies challenges in permissions, interoperability and the acquisition of terminals able to use multiple systems. The policy direction is toward hybrid networks, but implementation remains a procurement and integration problem.

For NATO forces, common access does not mean common control. The alliance should map which capabilities are nationally owned, commercially contracted, provider-managed or supplied by another ally. Plans should identify whether a service carries routine administrative traffic, operational data or a function whose interruption would constrain a time-sensitive mission. This mapping supports realistic priority rules and crisis consultation.

Provider concentration creates strategic exposure even where capacity is distributed across thousands of satellites. If one company supplies a large share of user terminals, software, cloud interfaces or gateway capacity, switching may require new equipment and retraining. Europe and NATO can diversify over time, but new constellations and sovereign systems do not provide immediate one-for-one substitutes for an established network. The transition period itself must be managed.

Operational-security exposure also matters. Commercial systems can generate telemetry, billing, location and usage records. The collection, retention and handling of those data should be addressed through contract and technical design. Emissions, terminal signatures and account management may reveal patterns even where message content is encrypted. Protection therefore requires both communications security and disciplined operational use.

Alliance assurance also depends on data handling. Commercial providers may hold service telemetry, account records, terminal locations or operational metadata even when message content is encrypted. Contract terms and technical controls should address access, retention, incident notification and cross-border processing. NATO exercises should test the practical release rules for allied data as well as network interoperability: a technically available path is not a usable fallback if the receiving unit lacks authority to access the information carried over it. These are operational conditions for commercial augmentation, not reasons to exclude private capacity.

Constraints and Counterarguments

Commercial scale and speed can strengthen resilience when dependence is deliberately managed.

Commercial infrastructure can increase resilience through distribution, rapid replacement and provider innovation. A constellation with many satellites may be harder to disrupt than a small number of exquisite military systems. Commercial imagery can make it more difficult for an adversary to conceal large movements, and competition among providers can reduce dependence when systems are genuinely interoperable.

Private systems may also field capability faster than government acquisition. GAO notes that US defense acquisition of new space systems has historically taken many years; its 2025 SATCOM review describes a shift toward integrated architectures with multiple access paths. Commercial procurement can bridge this time gap and add capacity without requiring a state to own every component.

These advantages do not make commercial dependence inherently unsafe. The relevant question is whether the arrangement is designed for a military mission: predictable access, appropriate security, sufficient capacity, priority under stress, clear governance and an operationally usable alternative. Risk rises when procurement treats a best-effort service as assured, or when a commercial tool becomes indispensable before the force has established policy and redundancy.

Sustainability

Long-term assurance depends on viable capacity, replacement, funding and continuity across providers.

A sustainable military architecture cannot assume that commercial capacity will always be available at the same price, service level or political conditions. Providers make investment decisions across civilian and government markets; satellites and gateways require replacement; launch capacity, spectrum, ground infrastructure, skilled labour and supply chains constrain expansion. During a major conflict, multiple states and commercial customers may compete for the same bandwidth and technical support.

Governments can reduce exposure through multi-year contracts, reserved capacity, government-owned or allied systems, diverse suppliers and funding for interoperable terminals. These measures impose recurring costs and may duplicate commercial capability. The case for sovereignty is strongest for functions where interruption would create a serious operational effect and no timely substitute exists; it is weaker for services that can be paused or replaced without affecting command.

The military should therefore measure sustainability by the number of mission pathways that remain usable under realistic disruption, the time required to switch, the capacity available after loss of a provider, and whether command can continue in a degraded mode. Satellite counts, terminal inventories and contract values are inputs, not evidence of continuity.

The overall assessment is that commercial space and digital infrastructure have become part of the operational fabric of modern military C2. Their distribution can improve resilience, but the conditions of access remain divided among military users, providers and governments. NATO and national forces should integrate commercial services while retaining the capacity to operate, communicate and exercise command when a provider, policy or network path is unavailable. The decisive measure is not ownership alone; it is whether the military can preserve command options under crisis conditions.

A continuity review should record recovery time, switch time, minimum capacity after a provider loss, percentage of critical users with compatible alternate terminals and the missions that can continue in degraded mode. These measures should be repeated after significant software, contract or force-structure changes. They give planners a more direct view of operational assurance than satellite counts or nominal bandwidth. The same review should identify which functions depend on commercial support by design and which have become dependent through habit, so that investment is directed toward genuine command risks.