Tomorrow's Affairs

Analysis of today
Assessment of tomorrow

By: Tomorrow's Affairs Staff

Who controls satellite links in a crisis?

Finnish companies Nokia, a telecommunications equipment manufacturer, and ICEYE, a satellite manufacturer, announced on 1 October that they will develop communications systems that countries can own and operate.

The offer covers satellites, ground stations and user devices, with the first launches expected in 2028.

The systems are intended for the armed forces, border services and emergency services, for whom any interruption to terrestrial networks can make operations or civilian rescue efforts impossible.

The two companies offer countries the ability to decide how to use the link without depending on the terms of a foreign commercial operator.

How extensive this independence will ultimately be depends on the division of labour and powers in future contracts, as well as on the ability of government agencies to manage the equipment they purchase.

Who can limit the state's satellite links?

By purchasing services from a satellite operator, the government can quickly establish connectivity without having to build and maintain its own network. The costs of the existing network are covered by subscriptions from multiple users, and the state contracts the service according to its needs.

The contract must specify in which territory and for which tasks the connection may be used, how many users can connect simultaneously, and how much data they may send and receive.

These conditions are particularly important when the operations of the armed forces or rescue services depend on the connection.

During a flood, teams on the ground must communicate with hospitals and aid distribution centres, while military units must receive operational orders and data in the field.

> The state must determine in advance the terms under which the operator may restrict or suspend the service

The state must determine in advance the terms under which the operator may restrict or suspend the service, as any interruption could endanger personnel on the ground.

ICEYE envisages three operational models: a dedicated satellite network for a single state, a shared network for allies and a provider-hosted network in which the state reportedly retains control over network access and data transmission. The company states that sovereign control is preserved in all three models, with data passing exclusively through approved national or allied infrastructure.

The published details do not specify the precise scope of autonomous state decision-making, nor which network management functions would be carried out by the state and which by the supplier.

When evaluating such an offer, it is essential to determine whether the state can independently connect users, direct bandwidth to priority operational areas, and maintain continuity of service if the supplier's specialists are unavailable.

A government may own the physical infrastructure yet remain entirely reliant on the supplier to operate it.

Reserved capacity incurs costs even when it is not in use

A state-owned network requires continuous funding for ground stations, cyber security, and the maintenance and replacement of satellites.

Trained personnel are needed to operate the infrastructure and resolve faults. If the budget covers procurement and launch but underestimates subsequent operating expenditure, the government risks being left with a system that lacks sufficient resources to operate reliably.

The scale of such capital commitments is illustrated by the European IRIS² programme, designed for secure governmental and commercial communications.

The 12-year concession contract for the construction and operation of the IRIS² constellation, signed in December 2024, is valued at €10.6 billion and financed through a combination of public and private capital.

This benchmark demonstrates the level of expenditure required to deploy such an architecture.

The proposal from Nokia and ICEYE covers discrete national systems, the pricing of which has not yet been disclosed.

> For smaller states, maintaining an independent network may prove disproportionately costly relative to their needs

For smaller states, maintaining an independent network may prove disproportionately costly relative to their needs.

Governments will need to determine which critical services require the highest level of security and which can rely on commercial alternatives.

Extending expensive, dedicated infrastructure to all public users could deplete funds needed for contingency equipment and for training the personnel on whom public safety directly depends.

The state pays for capacity reserved for its agencies even when it is idle, as the operator must guarantee availability and cannot commercialise that capacity elsewhere.

This capacity supports routine command and control, border surveillance and remote public administration, as well as operational resilience during outages of terrestrial infrastructure; the state must therefore secure appropriations for continual readiness, irrespective of actual utilisation.

Who receives the satellite connection everyone is seeking?

The European Union already provides an operational precedent for pooling existing capacity.

The GOVSATCOM programme, which supplies public authorities with secure satellite communications, began initial operations in January 2026. In March, the EU Agency for the Space Programme (EUSPA) announced that Cyprus had become the first operational user of its services, drawing on Greek sovereign capacity provided by the satellite operator Hellas Sat.

The initial offering pools capacity contributed by France, Greece, Italy, Luxembourg and Spain.

Through such cooperation, a state can secure protected communications without procuring a dedicated national constellation, but it must comply with common protocols on capacity allocation.

Under EU regulations, a high-priority operational request may, subject to prescribed criteria, trigger the suspension of a lower-priority service where necessary to release sufficient capacity.

These rules determine which transmissions take precedence when aggregate demand exceeds network throughput.

In the absence of clear rules, concurrent demands from multiple sovereign states risk precipitating diplomatic friction

A government integrating into a shared framework accepts that, in a contingency, a user from another member state may be given priority.

The underlying agreement must define how operational urgency is determined, designate the competent decision-making authority and specify how an agency whose service is limited is notified.

In the absence of clear rules, concurrent demands from multiple sovereign states risk precipitating diplomatic friction precisely when operational services require rapid decisions.

For states with modest defence budgets, a joint network remains compelling because it provides access to architecture that would otherwise be prohibitively expensive to procure independently.

Their standing within such a framework will ultimately depend on how rigorously and comprehensively the rules are defined in advance when several participants seek emergency capacity simultaneously.

The owner of the satellite can remain tied to the manufacturer

The British example shows how ownership and operational management can be separated.

In February 2023, the Ministry of Defence awarded Babcock a six-year contract to manage the armed forces' Skynet communications system.

Babcock and its industrial partners assumed responsibility for operating the ministry's satellites and ground stations, and for integrating new user equipment.

The state may appoint commercial contractors to operate its dedicated network, subject to clearly defined contractual powers and robust regulatory oversight.

Government specialists must retain access to all data required to audit operations, as well as the expertise needed to evaluate the operational risks of any hardware remediation or software modification.

A formal business continuity plan is also essential in case the contractor defaults on its obligations.

A cyberattack on Viasat's KA-SAT network, for which the EU attributed responsibility to Russia, caused widespread communications outages in Ukraine

Dependence on a single original manufacturer is particularly evident when replacement components, servicing or software patches can only be supplied by that manufacturer.

The government then has little commercial leverage to switch suppliers or challenge ongoing maintenance charges.

Unrestricted access to technical data packages, training for sovereign personnel and provisions for an orderly transfer of operations on contractual expiry must be secured before procurement.

A cyberattack on Viasat's KA-SAT network on 24 February 2022, for which the European Union attributed responsibility to Russia, caused widespread communications outages in Ukraine and disrupted critical infrastructure and civilian users in several EU member states.

The incident demonstrated how a wartime offensive targeting infrastructure in one state can undermine public authorities and essential services across borders, regardless of how rigorously network access protocols are defined.

Operational resilience exercises must rigorously test how quickly the armed forces and emergency services can fail over to redundant communications links following an outage and re-establish contact with deployed units and frontline personnel.

How much governments are willing to pay for independence

The most likely trajectory is a combination of commercial services with dedicated links for the most critical operations.

The joint offer from Nokia and ICEYE, designed to complement existing networks, exemplifies this approach.

For emerging European market entrants, government procurement contracts could become the financial foundation of their industrial development

The high costs of standalone systems will incentivise joint procurement, while states pursuing strategic autonomy will need to commit internal expertise and funding to operational functions previously outsourced to commercial operators.

Such demand could also unlock commercial opportunities for specialised manufacturers that lack the balance sheet strength to finance global networks for large numbers of commercial users.

Provided they demonstrate the required range and reliability, they can generate sustainable revenue by designing and supporting state-owned systems.

For emerging European market entrants, government procurement contracts could become the financial foundation of their industrial development, contingent on public authorities awarding multi-year commitments that justify upfront capital expenditure.

Ultimately, the scale and duration of these public-sector awards will determine how many independent suppliers remain viable, and the extent of sovereign choice governments that retain over their critical space communications.