The RETN Decision: When Internet Routing Becomes a Question of National Security

A U.S. final determination on network provider RETN puts internet transit, supply-chain risk and digital diplomacy in focus. The challenge is to strengthen security while preserving resilient and accountable connectivity.

Vladimir Tsakanyan, Ph.D. · Center for Cyber Diplomacy and International Security

November 27, 2026

Cover image: AI-generated conceptual illustration; it does not depict a specific network or facility.

The physical internet is often treated as neutral infrastructure: cables, routers and data centers moving information between people and institutions. Yet the companies that connect those networks operate under national laws, own or lease infrastructure across borders, and make decisions that can affect the availability and routing of international traffic. A new U.S. action involving network provider RETN shows how those commercial relationships are becoming matters of national security policy.

On November 27, 2026, the U.S. Department of Commerce placed a notice of final determination concerning RETN US LLC on public inspection. The Bureau of Industry and Security (BIS) said covered transactions involving RETN posed risks under the government's information and communications technology and services framework. The notice is scheduled for formal Federal Register publication on December 1; it is a notice of an issued determination, not a proposal for a new law. [1]

The central question is larger than any one company: how can governments reduce risks in essential connectivity without making international networks less resilient, less competitive or less open? The answer requires both a clear account of what the government has decided and humility about what its short public notice does not establish.

What the decision actually says

The notice defines RETN to include RETN US LLC together with its affiliates, subsidiaries and parent companies. It describes prohibitions covering specified information and communications technology transactions in the United States or with U.S. persons, including internet connectivity, private networking, cloud or data-center interconnection, and distributed denial-of-service mitigation services. The internet connectivity category includes

IP transit, peering, remote internet exchange access and border gateway protocol routing services. [1]

The notice requires RETN and covered successors or assignees to notify U.S.-person customers by December 2, 2026. It sets January 1, 2027 for terminating services to U.S. persons, removing covered equipment from U.S. networks and ceasing the prohibited transactions. The notice also requires evidence of compliance. Its written deadlines use the abbreviation “EDT” even though the dates fall in winter; affected organizations should check the official text and any clarification rather than assume a time conversion. [1]

An important footnote limits the scope: the determination does not apply to RETN-owned or operated submarine cable network infrastructure, if any, to the extent that infrastructure is subject to Federal Communications Commission regulation under the cited authorities. That qualification matters. The notice should not be summarized as an order to remove every cable connected to RETN or as a global ban on all of the company’s activities. [1]

The public document gives the government’s conclusion that the transactions present undue and unacceptable risks, but it does not describe a specific cyber intrusion or publish a detailed technical account of misconduct by RETN. Reuters reported the decision on November 27 and said its attempts to reach the company for comment were not immediately successful. Neither the notice nor that report establishes that RETN caused a particular breach or that internet service has already been disrupted. [1] [2]

Why transit belongs in the security conversation

Ordinary users rarely choose the wholesale providers that carry their traffic. A local access provider may buy transit from other networks, exchange traffic with peers at an internet exchange, or depend on a chain of contractors for capacity between cities and countries. A seemingly local service can therefore rely on several commercial relationships that its customers never see.

That creates legitimate security questions. Operators need to know which suppliers can administer infrastructure, how network changes are controlled, where their traffic may travel and how quickly service can be restored if a connection is lost. The risks differ with each service and contract. A provider that transports encrypted packets, for example, does not automatically possess the contents of those communications, although routing, availability and other information may still matter.

The Border Gateway Protocol, or BGP, is one of the mechanisms networks use to exchange information about routes. Routing decisions can reflect business relationships as well as technical reachability. NIST has documented the risks of erroneous or malicious route announcements and described route-origin validation as one way to improve routing integrity. Such measures help address specific routing threats; they do not by themselves

verify every provider, encrypt content or eliminate operational risk. [3]

The RETN notice cites BGP routing as one of the covered services, but it does not identify a BGP hijack as the reason for its decision. That distinction is essential: a general weakness in internet routing is not evidence of wrongdoing by a particular operator. The policy issue is how to manage exposure to providers and infrastructure before a disruption occurs, while preserving a standard of evidence for company-specific claims.

An older policy tool applied to a different layer

The determination rests on Executive Order 13873, issued in May 2019, and the implementing ICTS rules. The order established a national emergency framework for reviewing certain technology and services transactions associated with foreign-adversary risk. It authorized the Commerce secretary to prohibit transactions or consider mitigation measures under the stated conditions. The new notice applies that existing authority to a particular set of transactions; it does not create the original framework. [1] [4]

There is a historical parallel in telecommunications regulation. In October 2021, the FCC revoked China Telecom Americas' authority to provide certain domestic and international telecommunications services, citing national security and law-enforcement concerns. That decision involved the FCC's own carrier-authorization powers and an extensive proceeding. It is a useful comparison in how security concerns can reshape connectivity, not proof that the agencies made the same findings about RETN. [5]

The distinction between authorities matters for accountability. A carrier-license proceeding, a transaction-specific ICTS determination, an export control and a sanctions designation have different legal triggers and consequences. Collapsing them into the phrase "a cyber ban" conceals who is regulated, what is restricted and what evidence is publicly available. It can also encourage affected organizations to make operational decisions without understanding the actual text.

What the European comparison adds

The United States is not alone in treating technology supply chains as a security concern. In February 2026, the European Commission said the NIS Cooperation Group had adopted an ICT Supply Chain Security Toolbox developed by member states with the Commission and the EU Agency for Cybersecurity. The Commission described the measures as voluntary tools that countries can adapt to their circumstances; the accompanying risk assessments addressed connected vehicles and detection equipment. [6]

The European toolbox and the RETN determination are not equivalent instruments. The first is a set of measures supporting risk assessment across supply chains; the second is a U.S. company-specific final determination. Their shared significance is the policy shift toward examining dependencies across an entire service chain, rather than treating security as a

property of a single device.

Governments also face different pressures. A concentrated market can give a small number of operators disproportionate access to traffic and operational control. Replacing a provider may reduce one risk while leaving customers more dependent on another. The appropriate balance will differ by geography, service, available alternatives and the sensitivity of the systems involved. No single ownership label or technical control resolves those questions on its own.

The hidden cost of changing a route

A compliance deadline is a starting point for a complex migration. An enterprise may know its direct carrier while lacking a clear view of subcontracted circuits, colocation providers, network-exchange arrangements and backup routes. The first task is therefore an inventory of affected services and contractual relationships, followed by confirmation of which relationships actually fall within the published determination.

The next task is to test alternatives. Two connections sold by different providers may still share a building, fiber conduit, power supply or upstream carrier. A transition plan should consider physical diversity, available capacity, routing policies, recovery procedures and the ability to support essential operations if a planned cutover fails. These are general resilience measures; the public record reviewed here does not establish RETN’s particular customers or routes.

Governments have an interest in the quality of that transition. Abrupt changes can create operational problems for customers who are themselves critical-service providers. Clear guidance, a channel for case-specific questions and coordination with affected regulators can reduce uncertainty while preserving the security objective. Where legitimate, time-limited arrangements may be worth assessing under the applicable authorities, but the notice itself does not announce a general extension or exemption beyond its stated footnote.

Security, evidence and due process

The case illustrates a recurring tension in cybersecurity policy. Intelligence about a potential risk may be sensitive, but affected companies and the public still need enough information to understand the decision and assess its consequences. Public explanations can distinguish classified sources and methods from the nature of the concern, the relevant services and the practical path to compliance.

Good governance also requires a fair process. The company’s position, the possibility of review under applicable law, and the difference between a risk assessment and proof of an actual attack all deserve attention. The public notice does not provide a detailed account of RETN’s response or the underlying evidence. Until more is available, attributing espionage,

sabotage or control by a particular government would go beyond the record presented here.

A sound policy should be evaluated against measurable outcomes. Did affected customers receive timely notice? Were alternative routes genuinely diverse? Did the change reduce identified exposure without creating avoidable outages or excessive concentration? Were any compliance difficulties resolved transparently? These questions turn an announcement into a test of implementation rather than a symbolic contest over which country controls the internet.

The diplomatic dimension

Connectivity crosses borders even when legal authority does not. A provider may operate through multiple jurisdictions, while customers, exchange points and upstream networks may be elsewhere. A unilateral measure can therefore require coordination among regulators and operators that do not share identical security standards or legal obligations. Effective diplomacy means explaining the scope of a measure, protecting legitimate confidentiality and helping partners understand operational consequences.

The broader goal should be dependable interconnection with credible safeguards. That includes technical work on routing integrity, diversified infrastructure, incident coordination and clear commercial responsibilities. It also includes disciplined public language: a network-security decision can be consequential without proving that a specific attack occurred or predicting an imminent internet shutdown.

The RETN determination makes the politics of an often invisible layer of the internet unusually visible. Its long-term significance will depend less on the headline than on implementation: whether affected parties can make an orderly transition, whether the security rationale can be assessed, and whether governments and operators invest in resilient alternatives. The most durable form of digital sovereignty is not isolation; it is the ability to understand, govern and recover from dependence on others.

Sources and links

[1] U.S. Bureau of Industry and Security, Notice of Final Determination: RETN US LLC, Case ICTS-2025-006, filed for public inspection November 27, 2026

https://public-inspection.federalregister.gov/2026-24367.pdf

[2] Reuters, U.S. government bars bandwidth provider RETN from American networks, November 27, 2026

https://www.reuters.com/business/media-telecom/us-government-bars-bandwidth-provider-retn-american-networks-2026-11-27/

[3] NIST, Protecting the Integrity of Internet Routing: BGP Route Origin Validation, SP 1800-14

https://csrc.nist.gov/pubs/sp/1800/14/final

[4] Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain, May 15, 2019

https://www.govinfo.gov/content/pkg/FR-2019-05-17/pdf/2019-10538.pdf

[5] Federal Communications Commission, FCC Revokes China Telecom Americas' Authority, October 26, 2021

https://docs.fcc.gov/public/attachments/DOC-376902A1.pdf

[6] European Commission, ICT supply chain security: EU adopts a toolbox to mitigate risks, February 13, 2026

https://digital-strategy.ec.europa.eu/en/news/ict-supply-chain-security-eu-adopts-toolbox-mitigate-risks

Read the original article online

https://cybercenter.space/insights/retn-us-network-restrictions-internet-routing-cyber-diplomacy-2026/