WESTERN HEMISPHERE READINESS SERIES

HRS RESILIENCE FOUNDATION

SECTOR READINESS ASSESSMENT 01

Telecommunications & Digital Infrastructure

Sector Readiness, Continuity and Strategic Dependency

PUBLICATION TYPE	PRIMARY ENVIRONMENT	EDITION
Independent sector readiness assessment	Brazil, with Western Hemisphere applicability	August 2026

SERIES POSITION	AUTHOR	INSTITUTION
Sector Readiness Assessment 01	André Vieira	HRS Resilience Foundation

CONTENTS

About this series. The Western Hemisphere Readiness Series applies the HRS Readiness Cycle — Detect, Assess, Decide, Coordinate, Deploy, Sustain, Learn — to critical sectors across the Americas. Sector Readiness Assessment 01 is the fifth publication in the HRS Resilience Foundation's body of original research, following Strategic Report 01, Policy Brief 01, Technical Paper 01, and Country Readiness Assessment 01 — Brazil.

EXECUTIVE SUMMARY

Telecommunications & Digital Infrastructure

Telecommunications and digital infrastructure have become foundational to the continuity of modern societies. Government operations, emergency response, financial services, healthcare delivery, transportation, energy systems, logistics, commercial activity, and public communications increasingly depend upon interconnected digital networks.

The resilience of this environment cannot be measured solely by network availability, cybersecurity controls, or the number of physical connections. A resilient digital environment must also possess the capacity to detect disruption, assess consequences, make timely decisions, coordinate across institutions, deploy alternative capacity, sustain essential functions, and learn from failure.

The HRS Resilience Foundation applies its Readiness Cycle — Detect, Assess, Decide, Coordinate, Deploy, Sustain, Learn — to the telecommunications and digital infrastructure environment. The assessment examines six interconnected layers: physical connectivity; international connectivity; digital infrastructure and data centers; wireless infrastructure and 5G; cyber and operational resilience; and institutional and supply-chain dependencies.

THE HRS PROPOSITION

Digital resilience is not the absence of failure. It is the capacity of a system to continue essential functions, adapt under stress, recover from disruption, and improve before the next disruption occurs.

Data centers receive specific treatment because they increasingly connect telecommunications, computing, cloud services, energy, cooling, physical security, cybersecurity, and international connectivity. ANATEL has incorporated data centers, cloud computing, and submarine cables into strategic telecommunications planning and has identified data-center security and resilience as regulatory concerns.

The objective is not to identify political adversaries or assign blame. It is to establish a practical framework — built to remain valid across a 50-year horizon, independent of any single technology cycle or administration — through which governments, infrastructure operators, investors, and institutional decision-makers can identify critical dependencies and strengthen the ability of essential digital systems to remain functional under stress.

Five Core Findings

- **Communications infrastructure is a cross-sector dependency.** CISA identifies communications networks as supporting energy, transportation, water, emergency services, information technology, and financial services.
- **Redundancy must be tested for independence.** Multiple connections do not necessarily constitute effective redundancy when they share physical, power, technology, geographic, or maintenance dependencies.
- **Data centers are part of digital resilience.** Their continuity depends on connectivity, electricity, cooling, equipment, skilled personnel, cybersecurity, and recovery architecture. NTIA and DOE identify these dependencies as material to secure and resilient data-center growth.

- **International connectivity is strategic infrastructure.** The U.S. Department of State states that undersea cables carry more than 95 percent of global digital traffic and that vendor, maintenance, and repair choices can create dependency and security risks.
- **Readiness is continuous.** The goal is not to eliminate every failure but to ensure that critical services can continue, recover, adapt, and improve after disruption.

SECTION 01

Purpose and Scope

The purpose of Sector Readiness Assessment 01 is to examine the resilience and operational readiness of telecommunications and digital infrastructure through the HRS Readiness Cycle.

The assessment uses Brazil as its primary analytical environment while developing a methodology applicable to other countries and sectors throughout the Western Hemisphere.

The study is not a technical security audit of individual companies, networks, facilities, or vendors, nor an assessment of the intentions of governments or commercial organizations. It examines structural characteristics that may increase or reduce sector-level resilience: concentration, dependency, substitutability, redundancy, recovery capability, geographic exposure, supply-chain dependence, institutional coordination, cyber resilience, physical resilience, and cross-sector interdependence.

> *Can the telecommunications and digital infrastructure sector sustain essential functions when exposed to disruption, dependency, degraded operating conditions, or cascading failure?*

HRS treats national sovereignty over infrastructure, technology, and international-partnership decisions as a foundational premise of this methodology, not a variable to be assessed. The purpose of dependency analysis is to strengthen the capacity of sovereign institutions to identify their own exposures and expand their own range of options — never to prescribe which supplier, technology, or foreign partner a country should choose.

SECTION 02

Why Telecommunications and Digital Infrastructure Matter

CISA identifies communications as an interdependent critical-infrastructure environment. Communications networks support energy systems, transportation, water and wastewater, emergency services, information technology, and financial services; communications themselves depend on energy, IT, and transportation.

Brazil's national critical-infrastructure framework and ANATEL's PERT recognize the importance of protecting essential infrastructure and improving network resilience. ANATEL's 2025–2029 PERT incorporates data centers, cloud computing, submarine cables, cybersecurity, and other strategic digital-infrastructure issues into national planning.

> *The resilience of digital infrastructure must be evaluated according to the functions that depend upon it, not merely according to the infrastructure itself.*

Connectivity disruption → Loss or degradation of information flow → Operational disruption → Cross-sector dependency activation → Cascading institutional impact

SECTION 03

The HRS Sector Readiness Framework

The HRS Sector Readiness Assessment applies the seven-stage Readiness Cycle established in the Country Readiness Assessment 01. Each stage is treated as a functional readiness question rather than a numerical score.

FUNCTION	READINESS QUESTION	INDICATORS
Detect	Can institutions identify a material change early enough to matter?	Warning latency; monitoring coverage
Assess	Can fragmented information become a credible risk picture?	Fusion speed; confidence; consequence analysis
Decide	Are authorities and priorities clear?	Decision latency; delegated authority
Coordinate	Can responsible institutions act from a shared picture?	Interagency connectivity; role clarity
Deploy	Can alternative capacity move where required?	Mobilization time; logistics reach
Sustain	Can essential functions continue through disruption?	Effective redundancy; continuity
Learn	Does experience alter plans and investments?	After-action closure; corrective action

SECTION 04

Sector Architecture

For this assessment, telecommunications and digital infrastructure are treated as six interconnected layers.

LAYER	PRIMARY ELEMENTS	READINESS QUESTION
1. Physical Connectivity	Fiber; terrestrial routes; mobile/fixed networks; facilities	Can physical pathways remain available or be restored?
2. International Connectivity	Submarine cables; landing stations; gateways; satellite	Are international routes diverse and recoverable?
3. Digital Infrastructure	Data centers; cloud; exchanges; network management	Can computing and digital services continue if a major node fails?
4. Wireless Infrastructure	4G/5G; radio access; core functions; virtualization	Can wireless services remain secure, maintainable, and replaceable?
5. Cyber & Operational Resilience	Monitoring; response; recovery; emergency communications	Can operations continue during and after cyber disruption?
6. Institutional & Supply Chain	Operators; regulators; vendors; maintenance; equipment; workforce	Can dependencies be governed and substituted?

SECTION 05

Data Centers and Digital Infrastructure

Data centers are a convergence point between telecommunications, computing, cloud services, energy, cooling, physical security, cybersecurity, and data management. ANATEL's PERT 2025–2029 incorporates data centers and cloud computing into its strategic planning; ANATEL has also described data centers as part of the telecom infrastructure environment and has linked their regulation to security, resilience, and sustainability.

NTIA has identified data-center growth, supply-chain resilience, data security, power, broadband connectivity, workforce, and equipment as interconnected policy considerations. DOE's July 2026 draft transmission study identifies data centers as one contributor to accelerating electricity load growth and transmission needs.

Connectivity → Network → Data Center → Cloud / Computing → Digital Services → Critical Functions

The dependency also operates in reverse: data centers depend upon electricity, telecommunications, fiber, cooling, physical security, cybersecurity, equipment supply chains, skilled personnel, and geographic resilience.

HRS Data Center Readiness Questions

- **Connectivity** — multiple physically independent network paths.
- **Power** — continuity during electrical-system disruption.
- **Cooling** — continuity during cooling or utility disruption.
- **Geographic diversity** — sufficient distribution of critical workloads.
- **Cyber resilience** — detect, contain, recover, learn.
- **Physical resilience** — continuity during physical disruption.
- **Recovery** — restoration within an operationally acceptable period.

SECTION 06

International Connectivity and Undersea Cables

The U.S. Department of State states that undersea cables carry more than 95 percent of the world's digital traffic and notes that disruption can isolate countries, threaten national security, and create major economic damage. It also identifies vendor, maintenance, and repair choices as potential sources of dependency and insecurity.

ANATEL has identified submarine cables as critical to Brazil's international connectivity and has undertaken regulatory work addressing security, resilience, information requirements, and geographic concentration. In May 2026, ANATEL opened a 45-day public consultation on submarine-cable regulation, noting that approximately 99 percent of Brazil's international data traffic depends on this infrastructure and flagging the concentration of landing stations in a small number of locations — Fortaleza, Rio de Janeiro, Praia Grande, and Santos — as a structural exposure the consultation is intended to address.

The readiness question is therefore not simply whether a country possesses multiple cables.

> *How many genuinely independent pathways exist if a principal route becomes unavailable?*

Route diversity means multiple international paths. Effective route diversity means alternative paths do not share the same critical failure dependencies: the same landing location, terrestrial corridor, power infrastructure, geographic exposure, maintenance capability, or critical supplier.

HRS PROPOSITION

The objective is not simply more cables. It is more effective alternatives.

SECTION 07

Wireless Infrastructure and 5G

Wireless networks increasingly support consumers, businesses, government services, emergency communications, logistics, industrial systems, connected devices, transportation, and healthcare. The evolution toward 5G increases capacity and complexity.

The HRS assessment does not evaluate 5G exclusively according to performance. It evaluates the structural characteristics that determine whether the network can remain operational and recoverable.

- **Vendor concentration** — is a critical function concentrated in a limited supplier set?
- **Supply-chain resilience** — can critical components be sourced or replaced under disruption?
- **Software dependency** — can essential functions continue if updates or support are interrupted?
- **Network architecture** — are critical functions sufficiently segmented and recoverable?
- **Cybersecurity** — can the network detect, contain, and recover?
- **Interoperability** — can alternatives be introduced without unacceptable disruption?
- **Maintainability** — is qualified technical support available over the lifecycle?
- **Replaceability** — can high-consequence dependencies be replaced in acceptable time?

SECTION 08

Strategic Technology Dependency

Technology dependency becomes strategically relevant when replacing a supplier, technology, component, software platform, or service would require disproportionate time, cost, technical capacity, or institutional disruption.

DIMENSION	CORE QUESTION
Concentration	How much depends on one supplier, route, technology, facility, or geographic area?
Substitutability	Can the dependency be replaced within an acceptable period?
Recoverability	Is there a credible restoration pathway?
Control	Does the responsible institution have visibility and authority?
Cascading Impact	Would failure materially affect other essential functions?

> *The framework does not treat foreign ownership or foreign technology as automatically harmful. The issue is dependency and resilience, not nationality alone.*

SECTION 09

Cyber and Operational Resilience

Cybersecurity is necessary but not sufficient. A resilient telecommunications system must be capable not only of preventing incidents, but of maintaining essential functions during and after an incident.

CISA's communications-infrastructure guidance emphasizes visibility and hardening, while its dependency framework emphasizes upstream and downstream relationships affecting communications resilience.

Prevent → Detect → Contain → Operate → Recover → Learn

A network that cannot operate during an incident may remain technically secure while being operationally ineffective.

- Can essential services continue if the primary control environment is degraded?
- Are emergency communications available through independent pathways?
- Can operators isolate affected systems without unnecessary secondary failures?
- Are restoration priorities established before a crisis?
- Can critical technical personnel operate under degraded communications?
- Are recovery exercises realistic?
- Do post-incident lessons produce assigned corrective action?

SECTION 10

Institutional Coordination

Telecommunications resilience cannot be achieved by operators alone. The operating environment includes regulators, providers, data-center operators, cloud providers, energy providers, emergency services, government agencies, infrastructure owners, cybersecurity organizations, and technical specialists.

Effectiveness depends on defined responsibilities, reliable communication channels, incident protocols, decision authority, information-sharing mechanisms, restoration priorities, and exercises. Brazil's critical-infrastructure framework and ANATEL initiatives provide an institutional foundation for this work.

FUNCTION	READINESS QUESTION
Ownership	Are critical responsibilities and decision rights known?
Information	Can relevant actors exchange actionable information quickly?
Authority	Are escalation thresholds and restoration priorities predetermined?
Interoperability	Can technical and institutional systems work across boundaries?
Exercises	Have coordination arrangements been tested?
Learning	Are corrective actions assigned, tracked, and verified?

SECTION 11

Cascading Failure

The most significant sector-level risk may not be the initial telecommunications failure. It may be the consequences that follow. CISA's dependency framework demonstrates why communications resilience must be analyzed across sectors.

Primary disruption → Loss of connectivity → Dependent-system degradation → Secondary operational effects → Institutional consequences

- **Energy** — communications depend on electricity while energy systems use communications for monitoring and control.
- **Emergency services** — dispatch, public warning, coordination, and field communications depend on network availability.
- **Financial services** — transactions and market operations depend on reliable communications.
- **Healthcare** — records, telehealth, laboratory systems, logistics, and emergency coordination can depend on connectivity.
- **Transportation** — ports, airports, traffic management, logistics platforms, and fleet systems depend increasingly on communications.
- **Data centers** — computing facilities depend on connectivity, electricity, cooling, equipment, physical security, and workforce.

SECTION 12

The HRS Strategic Dependency Test

The HRS Strategic Dependency Test converts broad concern about infrastructure dependency into a repeatable analytical process.

QUESTION	WHAT TO EXAMINE	READINESS SIGNAL
1. Concentration	Supplier, route, facility, technology, geography	Low concentration or justified mitigation
2. Substitutability	Availability and time for alternatives	Credible alternatives within acceptable time
3. Recovery	Repair, replacement, rerouting, restoration	Tested recovery pathway
4. Control	Visibility, authority, maintenance, governance	Clear accountability and access
5. Cascading Impact	Downstream critical functions	Known priorities and continuity measures

The output should identify Critical Dependencies, Material Dependencies, Manageable Dependencies, and Dependencies Requiring Further Assessment rather than create false numerical precision.

SECTION 13

Nominal Redundancy vs. Effective Redundancy

Nominal redundancy describes the existence of an apparent alternative. Effective redundancy describes an alternative that remains operational when the principal dependency fails.

Network A and Network B may appear independent while ultimately depending upon the same physical corridor, power infrastructure, landing station, software platform, supplier, or maintenance capability.

TEST	QUESTION
Physical independence	Do alternative routes avoid the same physical failure point?
Power independence	Can alternatives operate if the same electrical system fails?
Technology independence	Do alternatives avoid the same critical technology dependency?
Geographic independence	Can a localized event affect both alternatives?
Maintenance independence	Do alternatives depend on the same repair capability?
Operational independence	Can the alternative be activated without the failed system?

HRS PROPOSITION

More infrastructure does not automatically produce more resilience. Independence matters.

SECTION 14

Sector Readiness Profile

The HRS Sector Readiness Profile identifies readiness gaps rather than assigning political judgments or a single national score.

DIMENSION	CORE QUESTION	EXAMPLES OF EVIDENCE
Operational Readiness	Can essential functions continue under degraded conditions?	Continuity procedures; staffing; alternate capacity
Continuity Readiness	Can alternatives sustain essential services?	Effective redundancy; backup communications; alternate routes
Dependency Resilience	Can dependencies be bypassed, replaced, or recovered?	Supplier diversity; route diversity; substitution time
Recovery Capacity	Can service be restored within an acceptable period?	Repair capability; spares; recovery exercises
Institutional Coordination	Can actors coordinate effectively during disruption?	Roles; information-sharing; exercises; corrective action

SECTION 15

Priority Readiness Gaps

The following conditions merit particular attention in sector-level readiness planning.

- **Geographic concentration.** Critical connectivity concentrated in limited locations can create systemic exposure.
- **Shared infrastructure.** Apparently independent systems may depend upon common physical or digital infrastructure.
- **Supplier concentration.** High dependence on a limited number of suppliers can increase replacement difficulty.
- **Limited recovery capacity.** Sophisticated preventive controls do not automatically create rapid restoration capability.
- **Data-center concentration.** Growing computing concentration can create new dependencies involving power, cooling, connectivity, and geography.
- **International connectivity dependence.** Limited diversity of international routes can increase exposure to external disruption.
- **Cyber-physical interdependence.** Cyber incidents may produce physical or operational consequences, while physical disruptions may produce digital-system consequences.

SECTION 16

HRS Sector Resilience Improvement Framework

The purpose of an assessment should ultimately be improvement. HRS therefore proposes eight sequential actions.

1. Map Critical Dependencies — Identify infrastructure, services, suppliers, facilities, routes, technologies, and institutions upon which essential functions depend.
2. Identify Single Points of Failure — Determine where loss of one component could materially disrupt essential services.
3. Test Effective Redundancy — Determine whether alternative systems remain independent when primary dependencies fail.
4. Establish Recovery Priorities — Define which services must be restored first and what capabilities are required.
5. Strengthen Supply-Chain Resilience — Evaluate alternative suppliers, components, maintenance capacity, and technical expertise.
6. Develop Cross-Sector Continuity Plans — Ensure telecom continuity planning reflects energy, healthcare, finance, logistics, transportation, and government dependencies.
7. Exercise the System — Test readiness through realistic exercises rather than relying solely on written plans.
8. Measure and Improve — Feed lessons into investment, infrastructure design, governance, and training.

SECTION 17

Long-Term Readiness

Digital infrastructure decisions frequently create dependencies that remain in place for decades. A network deployed today may determine technology choices, supplier relationships, maintenance requirements, data architecture, workforce requirements, replacement costs, interoperability, and recovery options long after the original procurement decision.

HRS INSTITUTIONAL DESIGN PRINCIPLE

HRS builds its readiness frameworks for a 50-year application horizon. A framework designed only for the current technology cycle or the current administration is not a resilience framework — it is a temporary arrangement. The HRS Readiness Cycle is built to remain valid as suppliers, technologies, and political leadership change across generations, so that sovereign institutions — not any single foreign relationship or vendor — remain in control of their own resilience over time.

The objective should not simply be to build the most capable system available today. It should be to build a system that can remain adaptable, replaceable, recoverable, and resilient as technology and strategic conditions change.

- Resilience before efficiency alone — critical systems require redundancy and recovery capacity.
- Interoperability before lock-in — critical functions should not become unnecessarily dependent on a single technology path.
- Recoverability before optimism — restoration capability should be tested, not assumed.
- Evidence before symbolism — infrastructure decisions should be based on measurable consequence and dependency.
- Adaptation before permanence — frameworks should survive technological and political change.
- Effective redundancy before nominal redundancy — alternatives must be independently operable.

SECTION 18

Western Hemisphere Perspective

Although this assessment uses Brazil as its primary analytical environment, the methodology is applicable throughout the Western Hemisphere.

Digital infrastructure increasingly crosses national boundaries through submarine cables, cloud services, international telecommunications, satellite systems, technology supply chains, and data flows.

SOUTHCOM's 2026 posture identifies critical infrastructure, telecommunications, cyber, undersea activity, ports, and other strategic infrastructure as relevant to hemispheric security. Its 2026 Commander's Imperatives include strengthening hemispheric command and control and denying adversary footholds and undue influence in the Western Hemisphere.

Institutional analyses published in 2026 describe an intensifying contest over the region's digital layer specifically. Independent policy-research institutions have pointed to efforts to replace existing network equipment from certain vendors in the region and frame digital-network security as a precondition for deeper U.S.-hemispheric technology cooperation, including on data centers and cloud infrastructure. Consistent with the HRS methodology, this development is presented here as documented institutional positioning, not as an HRS judgment on any individual vendor, technology, or country.

HRS's own methodology does not adopt any government's position on vendor or partnership choices. Decisions about suppliers, technologies, and international partnerships remain the sovereign prerogative of each national government; the role of dependency analysis is to inform that decision-making capacity with evidence, not to substitute for it or steer it toward any particular outcome.

The HRS approach is complementary but distinct: it concentrates on the institutional conditions that allow digital systems to remain operational and recoverable, regardless of changes in political leadership or individual suppliers.

HRS PROPOSITION

Resilient national infrastructure contributes to resilient hemispheric infrastructure.

Trusted infrastructure should be assessed through ownership, governance, legal jurisdiction, access rights, software control, update mechanisms, data access, maintenance dependence, supply-chain concentration, substitutability, and recovery capability. This distinguishes ordinary commercial dependency from strategic dependency without assuming that every foreign technology or investment is inherently problematic.

SECTION 19

Conclusion

Telecommunications and digital infrastructure constitute a foundational layer of modern institutional and economic continuity.

Their resilience cannot be determined solely by network speed, cybersecurity maturity, infrastructure volume, or technological sophistication.

A resilient system must also possess effective redundancy, diversified dependencies, recoverable architecture, reliable international connectivity, resilient data-center infrastructure, secure technology supply chains, capable emergency communications, cross-sector coordination, and the institutional ability to learn from disruption.

THE HRS PROPOSITION

Digital resilience is not the absence of failure. It is the capacity of a system to continue essential functions, adapt under stress, recover from disruption, and improve before the next disruption occurs.

Detect → Assess → Decide → Coordinate → Deploy → Sustain → Learn

Applied consistently, this framework moves digital infrastructure planning beyond the question of whether systems are secure toward a more consequential question: are they ready?

METHODOLOGY, RESEARCH INTEGRITY AND LIMITATIONS

Methodology, Research Integrity and Limitations

This report is an original HRS Resilience Foundation synthesis based primarily on public official documents from U.S. and Brazilian government agencies, complemented by selected institutional research. Sources establish documented facts, current strategic priorities, regulatory developments, and sector context. The HRS analytical synthesis, Sector Readiness Profile, Strategic Dependency Test, Nominal-versus-Effective Redundancy distinction, and Sector Resilience Improvement Framework are original constructs for this publication.

The assessment uses Brazil as the principal analytical environment because ANATEL provides detailed public planning material concerning network infrastructure, submarine cables, data centers, cloud computing, cybersecurity, and connectivity.

The report does not use classified information or claim access to confidential intelligence. Where public evidence is insufficient, the report identifies an analytical question rather than asserting a fact.

No allegation against a specific private company, public official, political party, community, or foreign government should be inferred from a sector-level vulnerability analysis. Operational decisions require competent authorities, applicable law, evidence, and due process.

The report should therefore be understood as a public-source sector readiness assessment, not a classified threat assessment, compliance certification, engineering audit, or legal opinion.

Research Integrity

- Documented fact is grounded in authoritative source material.
- Analytical judgment is presented as HRS assessment rather than external fact.
- Scenario reasoning is not presented as evidence of current conditions.
- Sector exposure is not equated with criminality or malign intent.
- Foreign participation is evaluated through dependency and resilience criteria rather than nationality alone.
- Sovereignty is a starting premise, not a variable: dependency analysis exists to expand the range of options available to national decision-makers, not to prescribe outcomes.

SELECTED BIBLIOGRAPHY AND SOURCES

Sources

[1] Cybersecurity and Infrastructure Security Agency (CISA). Communications Systems — Infrastructure Dependency Primer. U.S. Department of Homeland Security.

[2] U.S. Department of State. United States International Cyberspace & Digital Policy Strategy — Line of Effort 3: Enhance Security and Resilience of Undersea Cables. 2024.

[3] National Telecommunications and Information Administration (NTIA). Request for Comments on Bolstering Data Center Growth, Resilience, and Security. U.S. Department of Commerce, September 4, 2024.

[4] U.S. Department of Energy, Office of Electricity. 2026 National Transmission Needs Study — Consultation Draft and accompanying materials. July 2026.

[5] Agência Nacional de Telecomunicações (ANATEL). Plano Estrutural de Redes de Telecomunicações (PERT) 2025–2029. Brazil.

[6] ANATEL. Anatel aprova Plano Estrutural de Redes de Telecomunicações (PERT), edição 2025–2029. August 7, 2025.

[7] ANATEL. Tomada de Subsídios — Regulatory Framework for Submarine Telecommunications Cables in Brazil. Opened May 26, 2026, under the 2025–2026 Regulatory Agenda; 45-day public consultation.

[8] ANATEL. Conselheiro defende sustentabilidade e segurança na regulação de data centers. October 10, 2025.

[9] U.S. Department of Defense. Materials concerning secure 5G communications and telecommunications supply-chain resilience.

[10] CISA. Enhanced Visibility and Hardening Guidance for Communications Infrastructure. December 2024.

[11] Gabinete de Segurança Institucional da Presidência da República. Segurança de Infraestruturas Críticas. Brazil.

[12] U.S. Southern Command. 2026 Posture Statement to Congress. March 2026.

[13] U.S. Southern Command. Commander's Imperatives. 2026.

[14] U.S. Southern Command. Denying Malign Influence and Securing the Hemisphere. 2026.

[15] Center for Strategic and International Studies (CSIS). The Shield of the Americas Gathering and an Amplified Strategy to Counter China in the Western Hemisphere. May 2026.

[16] CSIS. Ending the Strategic Vacuum: A U.S. Strategy for China in Latin America. Analysis series, 2024–2025.

[17] HRS Resilience Foundation. Strategic Report 01 — Health Security and Institutional Resilience in the Americas: From Preparedness to Operational Readiness. August 2026.

[18] HRS Resilience Foundation. Policy Brief 01 — Strengthening Regional Health Emergency Readiness in the Americas: From Early Warning to Action. August 2026.

[19] HRS Resilience Foundation. Technical Paper 01 — Building Resilient Health Supply Chains. August 2026.

[20] HRS Resilience Foundation. Country Readiness Assessment 01 — Brazil: Institutional Readiness, Critical Infrastructure and Health-Security Continuity. August 2026.

Suggested citation: HRS Resilience Foundation. *Sector Readiness Assessment 01 — Telecommunications & Digital Infrastructure: Sector Readiness, Continuity and Strategic Dependency.* Western Hemisphere Readiness Series. August 2026.

WESTERN HEMISPHERE READINESS SERIES

HRS Resilience Foundation

Independent research for institutional readiness, continuity, and 50-year resilience planning across the Western Hemisphere. The Western Hemisphere Readiness Series applies the HRS Readiness Cycle to critical sectors, translating public-source evidence into practical frameworks built to remain valid for governments, infrastructure operators, investors, and institutional decision-makers across changes in technology, suppliers, and political leadership.

SERIES TO DATE

SRA 01 — Telecommunications & Digital Infrastructure
SRA 02 — Data Centers, Cloud & AI Infrastructure
SRA 03 — Critical Minerals & Strategic Materials
SRA 04 — Rare Earths & Western Hemisphere Mineral Security
SRA 05 — Energy Security & Strategic Power Infrastructure
SRA 06 — Ports, Logistics & Maritime Infrastructure
SRA 07 — Food Security & Strategic Agricultural Resilience
SRA 08 — Pharmaceutical & Medical Supply Chains
SRA 09 — Advanced Manufacturing & Industrial Capacity
SRA 10 — Western Hemisphere Strategic Infrastructure & Resilience

André Vieira, MD

FOUNDER & CHAIRMAN, HRS RESILIENCE FOUNDATION