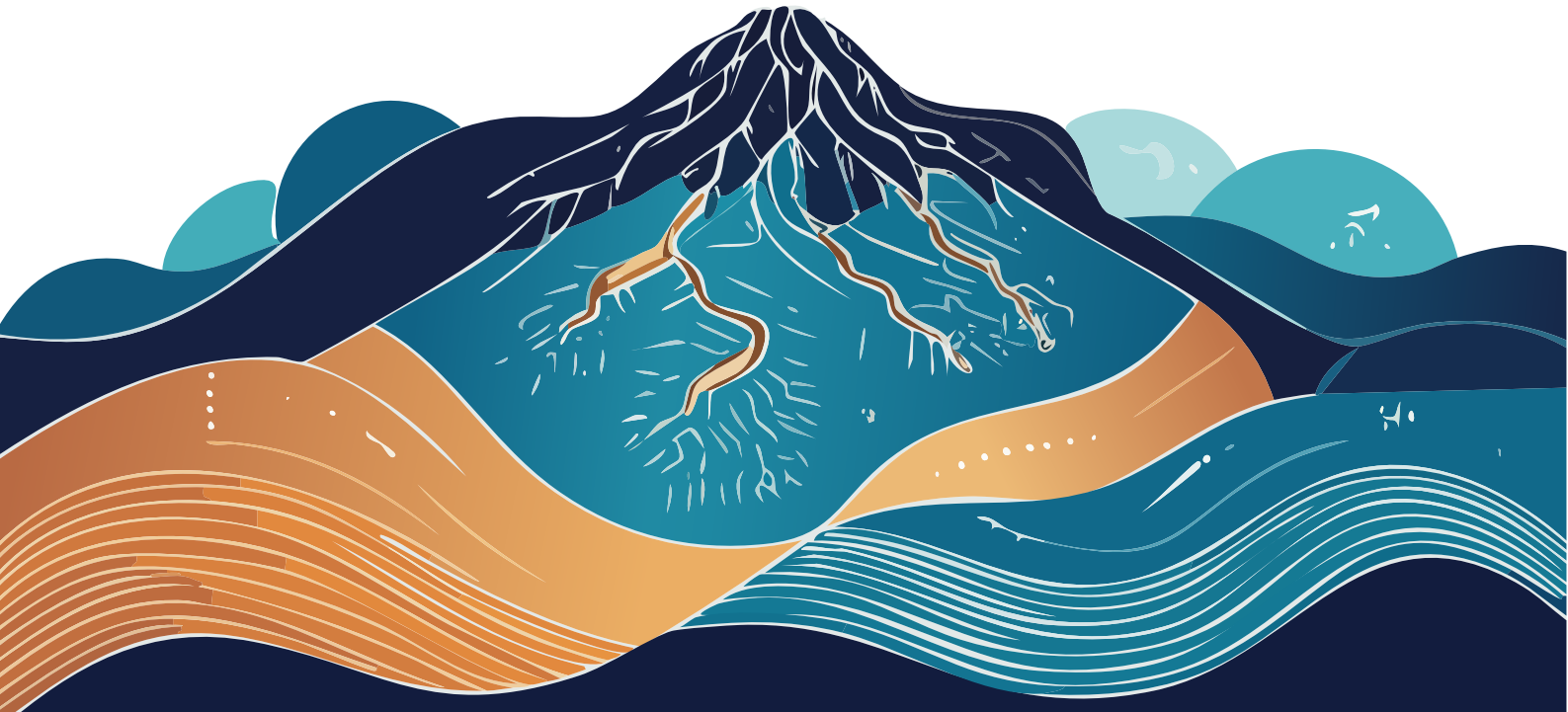
SocietĀs Partnerships

DECOLONIZING THE DIGITAL RESEARCH ECOSYSTEM

STRATEGIC PATHWAYS TO SOVEREIGN DATA INFRASTRUCTURE AND CONNECTIVITY IN THE GLOBAL SOUTH



societaspartnership.com

DECOLONIZING THE DIGITAL RESEARCH ECOSYSTEM: STRATEGIC PATHWAYS TO SOVEREIGN DATA INFRASTRUCTURE AND CONNECTIVITY IN THE GLOBAL SOUTH

INTRODUCTION: THE INFRASTRUCTURE PARADOX IN GLOBAL SCIENCE

Modern scientific endeavor is fundamentally reliant on a robust digital foundation. From high-performance computing and collaborative data sharing to real-time sensor networks and global academic partnerships, the digital infrastructure is the engine of contemporary research and innovation. It facilitates unprecedented collaboration, accelerates discovery, and democratizes access to knowledge. However, for many nations in the Global South, this increasing access to digital connectivity and data platforms has created a profound and often unseen paradox. While these tools ostensibly connect researchers and foster progress, their prevailing model of centralization, rooted in foreign-owned and controlled platforms, has paradoxically led to a new form of technological dependency, eroding national and institutional autonomy.

This report posits that a strategic shift is required to address this paradox. The imperative is to achieve a form of Digital Sovereignty—a concept that extends far beyond mere data regulation. In the context of research and innovation, digital sovereignty is the ability of a nation to control its own "digital destiny," including the data, hardware, and software on which its academic and scientific systems rely and which they create[1]. This capacity is not just about establishing firewalls or implementing local data storage laws; it is about fostering a homegrown technology industry and funding local innovation to build autonomous, resilient, and equitable digital ecosystems[1]. Building this sovereign infrastructure is an inherently geopolitical act. The concept of digital sovereignty is itself a contested and dynamic claim, functioning as a "discursive resource" in political struggles between nation-states, regional blocs like the European Union, and powerful corporate entities.[2] This framing demonstrates that the future of scientific infrastructure in the Global South is not a purely technical or legal challenge, but a fundamental struggle over power and self-determination.

The core thesis of this report is that the prevailing model of digital infrastructure in the Global South, characterized by a reliance on centralized, foreign-owned platforms, perpetuates data colonialism and stifles independent scientific innovation. To achieve true research autonomy, Global South nations must strategically leverage the intersection of next-generation connectivity and decentralized data architectures, supported by robust regional governance frameworks, South-South collaboration, and investments in local capacity. This report will first provide a critical analysis of the geopolitics of research infrastructure and the mechanisms of data colonialism. It will then explore the technological opportunities presented by a shift to decentralized architectures and next-generation connectivity. Finally, it will synthesize these findings into a comparative case analysis and a strategic framework for action.

THE GEOPOLITICS OF RESEARCH INFRASTRUCTURE: UNDERSTANDING DIGITAL AND DATA COLONIALISM

The current global digital landscape cannot be understood merely as a collection of networks and services; it must be viewed through a Socio-Technical Systems (STS) approach. This framework acknowledges that technology is not a neutral tool but is deeply intertwined with and shapes human capital, policy, economic structures, and geopolitical dynamics. From this perspective, the reliance of Global South nations on centralized, foreign-owned cloud infrastructure reveals a profound power asymmetry that echoes historical patterns of domination.

The central mechanism of this contemporary power dynamic is data colonialism, a new frontier of imperialism that combines the predatory extractive practices of historical colonialism with the abstract, ubiquitous quantification methods of modern computing[3]. This process is defined as the systematic appropriation of personal, social, and communal data by global corporations and states[4]. This appropriation can be understood as a form of "capitalist accumulation by dispossession"[5]. Much like historical colonizers treated land, resources, and bodies as raw materials "just there" for the taking, data colonialism treats social life itself as an open resource for extraction[3]. The process is normalized and legalized through mechanisms such as End-User-License-Agreements, which effectively dispossess the data producers of their right to own and control the resource they generate[5]. The data is then used to generate value and power[3].

Concrete examples of this dynamic are evident in both public and private sectors. The collection of DNA data from Indigenous peoples, for instance, has been critiqued as an extension of past colonial efforts, with concerns that researchers may use the data to further their careers rather than address the needs of the communities from which it was taken[5]. In urban environments, the deployment of surveillance technologies, such as predictive policing, has been shown to reinforce existing racial biases and societal inequalities, mirroring the historical legacies of apartheid and racial segregation in countries like South Africa[4]. Furthermore, the narrative of "benevolent" tech companies, which promote "free" connectivity initiatives in the name of "progress" and "connecting people," functions as a modern-day "civilizing mission"[6]. This narrative masks the true purpose of these initiatives, which is to design digital infrastructures that like any industry has monopolistic inclinations creating a strong societal dependency on their platforms, a sign of economic success from the part of the giant IT companies at the expense of centralization[6]. This technological lock-in makes it exceedingly difficult for any local, sovereign alternatives to emerge and compete, even if they could offer more equitable and empowering services. China has been the only other country capable of producing the type of companies able to compete U.S. tech companies. But such capability is due to its rising place as a superpower, its

massive population and rising aspirations.

The geopolitical contest for control over digital infrastructure is increasingly overt. Nations are becoming wary of relying on foreign technology for critical systems, a trend that has led to the fragmentation of the once-borderless cloud into national silos[7]. The fear of surveillance or foreign leverage is a central motivation for data localization laws[7]. However, a complex tension exists for many developing nations. While the security risks of using foreign-owned cloud infrastructure are clear—including potential espionage and the compromise of sensitive data—the appeal of these services is often overwhelming[8]. Developing countries frequently opt for foreign providers due to the imperative for rapid development, lower prices, and the provision of technical assistance that local alternatives cannot yet match[8]. This dynamic demonstrates that an appeal to security alone is insufficient to counter the powerful economic motivations driving these choices, highlighting the need for a more comprehensive approach that addresses both trust and development.

THE TECHNOLOGICAL SHIFT: OPPORTUNITIES FOR DECENTRALIZED ARCHITECTURES

The limitations of the centralized cloud model—including high latency in low-resource environments, the considerable cost of data transport to remote data centers, and the lack of local control over proprietary platforms—highlight the need for a fundamental shift in infrastructure design[7]. Emerging technologies, particularly in the realm of decentralized data architectures and next-generation connectivity, offer a strategic pathway toward a more sovereign and equitable research ecosystem.

Emerging Data Architectures: A Strategic Pivot

Decentralized data architectures represent a crucial departure from the traditional model of data aggregation. The core principle is to distribute data storage and processing across multiple nodes or systems, allowing each domain to manage its own data while ensuring organization-wide accessibility[9]. This approach is not merely a technical alternative but a strategic one that aligns with the principles of digital sovereignty. It empowers domain-specific teams, enhances resilience, fault tolerance, and promotes data localization and autonomy[9].

A prime example is Federated Learning, a distributed machine learning approach that keeps data on local devices or servers, sharing only model updates (like gradients or weights) with a central coordinator[11]. This method fundamentally addresses privacy and bandwidth constraints by preventing the transfer of raw, sensitive data[11]. It is particularly relevant for applications involving highly sensitive information, such as biomedical research and genomic studies, as it allows for collaborative model training across institutions without compromising data privacy[11].

Similarly, Edge Computing offers a complementary solution by processing data closer to its source, at the "edge" of the network[13]. This approach significantly reduces the latency and cost of transporting large volumes of data to a remote, centralized cloud, making it ideal for data-intensive applications like remote healthcare and agricultural monitoring[13].

However, the effective implementation of these decentralized technologies requires a complementary shift in governance. Simply adopting the technology is insufficient. The empowerment of domain-specific teams through decentralization can lead to "global standards" and "complex data integration"[9]. To overcome these challenges, a federated governance model must be established. This model defines clear, shared data governance policies and standards that can be applied across all domains, ensuring consistent security and quality while maintaining the

autonomy of individual teams[9]. The technological shift toward decentralization, therefore, necessitates a simultaneous and deliberate shift in political and institutional capacity to build the governance frameworks that make the technology work equitably and effectively.

Next-Generation Connectivity: The Crucial Enabler

These decentralized strategies are only viable when supported by a new generation of connectivity technologies that can overcome the limitations of traditional terrestrial networks.

- **6G Networks:** The sixth generation of wireless networks is envisioned as a foundational technology for decentralized systems, driven by a vision of ubiquitous intelligence and distributed data management[12]. 6G architecture is being designed to intelligently support a wide range of smart services that rely on collaborative learning and distributed data[16]. A critical component of this vision is the integration of Blockchain Technology (BCT), whose inherent properties of decentralization, transparency, and immutability are perfectly suited to enable federated resource sharing and secure data management in trust-less environments[17]. This convergence allows for the secure and private transfer of information without the need for a central, third-party authority[19].
- **Low Earth Orbit (LEO) Satellites**: LEO satellite constellations, operating at lower altitudes, provide the global, high-bandwidth, and low-latency connectivity needed to make edge computing solutions viable in remote and hard-to-reach areas[13]. These networks can cover regions that traditional terrestrial networks cannot, such as deserts and oceans, and provide crucial resilience in the event of natural disasters that disrupt ground-based infrastructure[14]. The rapid deployment and global reach of LEO satellites enable the extension of digital services, such as remote healthcare and micro-financing, to previously unconnected populations, thereby empowering location-sensitive edge computing and reducing reliance on a centralized cloud[13].

PATHWAYS TO SOVEREIGNTY: A COMPARATIVE CASE ANALYSIS

To move from theory to practice, this report presents a comparative analysis of three distinct models for achieving sovereign research infrastructure. Each model, while unique, offers valuable lessons on governance, funding, and collaboration. The analysis reveals that achieving digital sovereignty does not necessitate economic self-sufficiency; rather, the most successful models demonstrate the power of strategic interdependence and a phased approach to development. Sovereignty is not about isolation but about building the infrastructure and governance capacity to engage with the world on equitable terms.

Case 1: Building Regional Capacity – RedCLARA and the BELLA Programme

The BELLA Programme (Building the European Link to Latin America) is a powerful example of how strategic, inter-regional collaboration can create a sovereign asset. In partnership with the European Union and European National Research and Education Networks (NRENs), the program secured an Indefeasible Right of Use (IRU) of 40 optical channels on a direct transatlantic submarine cable between Latin America and Europe[25]. This strategic move provided "very high, cost-effective capacity, shorter routes and diversely stimulating data sharing"[25]. Instead of relying on commercial carriers that route traffic through the United States, RedCLARA and its partners now have a dedicated, long-term link for research and education[21]. This approach, funded through a mix of European and local contributions, allowed them to build a critical piece of infrastructure on their own terms, demonstrating that a strategic partnership can be a pathway to autonomy[24]. It will support 3,000 institutions, with the potential to expand to 12,000, and assist more than 65 million students[35].

Case 2: State-Led Strategy – The Indian Digital Public Infrastructure (DPI) Model

India's Digital Public Infrastructure (DPI), known as the India Stack, provides a blueprint for a state-led approach to digital sovereignty. The government built a foundational layer of open-source "digital public goods"[22], including a digital identity system (Aadhaar), a real-time payments platform (UPI), and a data exchange framework[22]. This foundational "plumbing for the Internet Age" has lowered the barrier to entry for domestic startups and catalyzed a vibrant fintech ecosystem[26]. By providing a level playing field and open, interoperable APIs, the India Stack has reduced market concentration risk and empowered private sector innovators to create value-added services at scale, while also driving massive

financial inclusion[26]. This model's success lies in its ability to act as a public enabler, fostering private-sector innovation and competition without centralizing control over the services themselves.

Case 3: Navigating Constraints – Lessons from African NRENs

African National Research and Education Networks (NRENs) face significant and pragmatic challenges, most notably the lack of funding to own their own connectivity infrastructure[27]. This challenge is compounded by the fact that commercial and public Internet Service Providers (ISPs) often see NRENs as competitors, making it difficult to forge partnerships[27]. However, this context has also led to innovative, on-the-ground strategies. The Zambian NREN (ZAMREN), for example, has built exemplary partnership models with public and private entities, including power and water utility companies, to gain access to their existing fiber optic backbones[27]. This strategy demonstrates that creativity, transparency, and the ability to demonstrate a clear public service mission can overcome major obstacles[27]. Furthermore, projects like AfricaConnect3, co-funded by the European Union and African partners, provide high-speed internet connectivity and digital services to African research and education communities, allowing NRENs to gradually build the infrastructure and human capacity necessary for future autonomy and resilience[23].

Other examples include South Atlantic Cable System (SACS), the first and only submarine fiber-optic cable to directly connect Africa (Angola) with South America (Brazil)[36]. The African Data Center Boom, a massive, ongoing investment in building high-capacity, carrier-neutral data centers directly on African soil, led by companies like Teraco (South Africa) and Africa Data Centres[37]. OpenStack, a free and open-source software platform for creating and managing private and public clouds[38]. Modular Open Source Identity Platform (MOSIP), born out of research in India, MOSIP is an open-source, "DPI in a box." It provides a robust, scalable, and free platform for countries to build their own national foundational identity systems, just like Aadhaar[39]. South Africa's Centre for High Performance Computing (CHPC), a world-class supercomputing facility located in Cape Town. It provides massive computational resources to researchers across South Africa and the entire Southern African Development Community (SADC) region[40].

A STRATEGIC FRAMEWORK FOR DECOLONIZING DIGITAL RESEARCH ECOSYSTEMS

Based on the theoretical critique and the practical lessons from the case studies, a comprehensive framework for decolonizing digital research ecosystems must be built upon a foundation that addresses the multifaceted nature of the challenge. The following PESTLE (Political, Economic, Sociological/Social, Technological, Environmental, and Legal factors) analysis provides a holistic summary of the enabling conditions and barriers, linking them to a strategic, multi-pillar framework for action.

Pillar 1: Policy and Governance Imperatives

To establish a truly sovereign digital ecosystem, policymakers must move beyond a reactive stance. This requires the creation of proactive legal frameworks that mandate data residency and enforce open standards and interoperability to prevent technological lock-in[1]. Governments should incentivize the adoption of decentralized and open-source platforms and create regulatory sandboxes for new technologies. Such policies should ensure that citizen-facing digital services do not become expensive, which would defeat the purpose of digitization[29].

Pillar 2: Investment Strategies and Sustainable Funding

The case studies demonstrate that sustainable funding models are essential. This requires leveraging a diverse portfolio of capital, including public investment, support from regional development banks, and strategic international partnerships for large-scale infrastructure projects like submarine cables and satellite constellations[23]. National Research and Education Networks (NRENs) play a crucial role as "demand aggregators," leveraging the collective buying power of universities and research institutions to secure lower prices for bandwidth and other services, a function that commercial ISPs (internet service providers) cannot provide[32].

Pillar 3: The Human and Social Capital Dimension

Investing in people is as critical as investing in hardware. A strategic approach requires building local expertise in infrastructure governance, maintenance, and the development of new applications, moving beyond a model of being mere consumers of foreign technology[31]. This includes fostering a new generation of researchers and technologists who can navigate the complexities of decentralized systems and contribute to open-source communities. From an ethical standpoint,

it is essential to build this capacity in a way that respects and empowers marginalized and Indigenous communities[33]. This requires adopting frameworks that prioritize relational principles like reciprocity, mutual benefit, and self-determination over simplistic notions of individual consent[34]. This ensures that the benefits of digital infrastructure and research are shared equitably and that data extraction does not perpetuate historical patterns of harm.

Pillar 4: Fostering South-South Collaboration

The success of a decolonized digital ecosystem depends on a critical mass of infrastructure and a shared knowledge base. Global South nations must actively foster collaboration and build shared infrastructure networks among themselves. The RedCLARA and BELLA Programme is a powerful blueprint for how collective action can secure a common asset and challenge the dominance of North-South data flows. Similarly, the India Stack model, by being open and replicable, provides a model for other nations to learn from and adapt, promoting a new form of South-South collaboration by example[22]. These efforts enable the Global South to forge a collective, sovereign future, where knowledge and infrastructure are shared on a basis of mutual trust and benefit.

CONCLUSION: FORGING EQUITABLE DIGITAL FUTURES

The current model of digital infrastructure presents a significant paradox for the Global South: increased access to global platforms often comes at the cost of national autonomy and the risk of data colonialism. The prevailing centralized model of data and network infrastructure is not a neutral development but a geopolitical reality that perpetuates historical and economic power imbalances. Resources in some cases won't be enough for some countries who aim at competing with established players, such as in the case of China vs the U.S. and established markets will compete fiercely to maintain their position. It is clear that government intervention is necessary for the Global South to decrease their dependence on data infrastructure and connectivity. The convergence of emerging connectivity technologies like LEO satellites and 6G with decentralized data architectures like federated and edge computing provides a viable technological pathway toward a more sovereign future. While investments are integral part of any strategy, governments and universities can opt for new forms of partnerships.

To realize this potential, a strategic, multi-pronged framework is required. It demands proactive policy and governance to ensure data residency and

interoperability. It necessitates diversified investment strategies and sustainable funding models to build and maintain critical infrastructure. Most importantly, it requires a commitment to building local human capital and adopting ethical frameworks that empower communities and ensure the equitable distribution of benefits. The path to decolonizing the digital research ecosystem is a long-term undertaking, requiring sustained political will and collaboration. By strategically building their own digital public infrastructure and fostering robust South-South collaboration, Global South nations can forge a new, equitable, and autonomous future for science, innovation, and development.

References

1. What is digital sovereignty and how are countries approaching it? | World Economic Forum, accessed September 23, 2025, https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/
2. Full article: Attributes of Digital Sovereignty: A Conceptual Framework, accessed September 23, 2025, https://www.tandfonline.com/doi/full/10.1080/14650045.2025.2521548
3. Nick Couldry and Ulises Mejias - Data colonialism: rethinking big ..., accessed September 23, 2025, https://eprints.lse.ac.uk/89511/1/Couldry_Data-colonialism_Accepted.pdf
4. Data Colonialism, Algorithmic Justice, and the Law: A Global South Perspective, accessed September 23, 2025, https://www.researchgate.net/publication/395544028_Data_Colonialism_Algorithmic_Justice_and_the_Law_A_Global_South_Perspective
5. Glossary: Data Colonialism - Critical Data Studies - Purdue University, accessed September 23, 2025, https://purdue.edu/critical-data-studies/collaborative-glossary/data-colonialism.php
6. An intellectual history of digital colonialism - Oxford Academic, accessed September 23, 2025, https://academic.oup.com/joc/advance-article/doi/10.1093/joc/jqaf003/8078024
7. AI geopolitics and data centres in the age of technological rivalry, accessed September 23, 2025, https://www.weforum.org/stories/2025/07/ai-geopolitics-data-centres-technological-rivalry/
8. An Overview of Global Cloud Competition - CSIS, accessed September 23, 2025, https://www.csis.org/analysis/overview-global-cloud-competition
9. Decentralized data architecture - Explanation & Examples | Secoda, accessed September 23, 2025, https://www.secoda.co/glossary/decentralized-data-architecture
10. Everything You Need to Know When Assessing Decentralized Data Architecture Skills, accessed September 23, 2025, https://www.alooba.com/skills/tools/data-engineering-infrastructure/decentralized-data-architecture/
11. How does federated learning differ from centralized learning? - Milvus, accessed September 23, 2025, https://milvus.io/ai-quick-reference/how-does-federated-learning-differ-from-centralized-learning
12. Federated Learning for 6G Networks: Navigating Privacy Benefits and Challenges, accessed September 23, 2025, https://www.researchgate.net/publication/386590290_Federated_Learning_for_6G_Networks_Navigating_Privacy_Benefits_and_Challenges
13. Edge computing solution - OneWeb, accessed September 23, 2025, https://oneweb.net/solutions/government/edge-computing-solution
14. Edge-Distributed IoT Services Assist the Economic Sustainability of LEO Satellite Constellation Construction - MDPI, accessed September 23, 2025, https://www.mdpi.com/2071-1050/16/4/1599
15. Centralized vs Federated Digital Data Transformations: Which Approach Will You Choose?, accessed September 23, 2025, https://infinitive.com/centralized-vs-federate-digital-transformations/
16. Split Federated Learning for 6G Enabled-Networks: Requirements, Challenges and Future Directions - TU Wien's reposiTUm, accessed September 23, 2025, https://repositum.tuwien.at/bitstream/20.500.12708/212429/1/Hafi-2023-Split%20Federated%20Learning%20for%206G%20Enabled-Networks%20Requirements%2C...-smur.pdf

17. The Convergence of Blockchain, IoT and 6G: Potential, Opportunities, Challenges and Research Roadmap - arXiv, accessed September 23, 2025, https://arxiv.org/abs/2109.03184

18. Blockchain and 6G-Enabled IoT - MDPI, accessed September 23, 2025, https://www.mdpi.com/2411-5134/7/4/109

19. Study the Blockchain-Based AI Data Security in 6G Networks - Nanotechnology Perceptions, accessed September 23, 2025, https://nano-ntp.com/index.php/nano/article/download/4563/3517/8764

20. Study the blockchain-based AI data security in 6G networks - ResearchGate, accessed September 23, 2025, https://www.researchgate.net/publication/393857176_Study_the_blockchain-based_AI_data_security_in_6G_networks

21. World Regions - Latin America - GÉANT, accessed September 23, 2025, https://www.geant3.archive.geant.org/pages/Network/worldregions-LatinAmerica.html

22. India Stack, accessed September 23, 2025, https://indiastack.org/

23. FAQs | AfricaConnect3, accessed September 23, 2025, https://africaconnect3.net/faqs/

24. BELLA II: Connecting the Digital Future of Latin America and the Caribbean - YouTube, accessed September 23, 2025, https://www.youtube.com/watch?v=JWfE0HXQpIY

25. BELLA - RedCLARA, accessed September 23, 2025, https://www.redclara.net/en/colaboracion/proyectos/red-e-infraestructura/bella

26. Digital Public Infrastructure as a Catalyst for Private Sector Innovation, accessed September 23, 2025, https://www.orfonline.org/research/digital-public-infrastructure-as-a-catalyst-for-private-sector-innovation

27. ZAMREN demonstrates NREN meaningful synergies with public and ..., accessed September 23, 2025, https://ubuntunet.net/connectivity/zamren-demonstrates-nren-meaningful-synergies-with-public-and-private-connectivity-infrastructure-owners-2/

28. The Americas Research and Education Networks (AMREN) - RedCLARA, accessed September 23, 2025, https://www.redclara.net/en/colaboracion/conozca/redes-de-investigacion-y-educacion-de-las-americas-amren

29. India stack---digital infrastructure as public good - ResearchGate, accessed September 23, 2025, https://www.researchgate.net/publication/336787723_India_stack---digital_infrastructure_as_public_good

30. Digital Public Infrastructure:, accessed September 23, 2025, https://dco.org/wp-content/uploads/2025/06/DPI-Policy-Paper.pdf

31. Impact case study (REF3) Page 1 Institution: Brunel University London Unit of Assessment, accessed September 23, 2025, https://results2021.ref.ac.uk/impact/0c45f2e6-54e3-4e69-bdc2-a2dc94f03e70/pdf

32. About NRENs - MAEEN NETWORK, accessed September 23, 2025, https://www.maeen.sa/en/about/nrens/

33. Indigenous Data | ARDC - Australian Research Data Commons, accessed September 23, 2025, https://ardc.edu.au/resource/indigenous-data/

34. Ethical Frameworks for AI and Indigenous Data Sovereignty. → Scenario, accessed September 23, 2025, https://prism.sustainability-directory.com/scenario/ethical-frameworks-for-ai-and-indigenous-data-sovereignty/

35. BELLA - Building the Europe Link to Latin America. (n.d.). International Partnerships. https://international-partnerships.ec.europa.eu/policies/programming/projects/bella-building-europe-link-latin-america_en

36. Angola Cables. (n.d.). SACS. Retrieved September 24, 2025, from https://www.angolacables.co.ao/sacs-cable-system-is-now-live/

37. Africa Data Centres. (n.d.). Home. Retrieved September 24, 2025, from https://www.africadatacentres.com/

38. OpenStack. (n.d.). What is OpenStack? Retrieved September 24, 2025, from https://www.openstack.org/ software/

39. Modular Open Source Identity Platform. (n.d.). Home. Retrieved September 24, 2025, from https://www.mosip.io/

40. Centre for High Performance Computing. (n.d.). About Us. Retrieved September 24, 2025, from https://www.chpc.ac.za/about-us/

Societās Partnerships

Societās helps universities foster excellence through internationalization by providing comprehensive assessments, strategic guidance, and effective implementation.

Prepared by

Carlos Vargas, M.Ed
Founder, **Societās Partnerships**
Panama
founder@societaspartnership.com
September 2025