The Weaponization of Digital Dependency

How Small States Can Protect their Digital Sovereignty amid Geopolitical Conflict

Ben Norton

Ph.D. student, International Relations Department, Tsinghua University

Abstract: This paper addresses the critical challenge faced by small countries in the Global South, and particularly Latin America, that seek to protect their digital sovereignty in an era of increasing technological dependence, geopolitical conflict, and great power rivalry between the United States and China. Recent infrastructure disruptions and documented cyber operations by major powers demonstrate that digital infrastructure has become a domain of economic, political, and military vulnerability. This article proposes a multi-pronged approach centered on diversifying technology partnerships, reducing dependency on US technological infrastructure, strengthening regional cooperation, and building domestic technical capacity to preserve independence, ensure strategic autonomy, and protect national security.

Keywords: *Digital sovereignty, technology, national security, Global South, South-South cooperation, Latin America*

The Problem of Digital Dependency

In the 21st century, state institutions, military installations, communications systems, private enterprises, healthcare systems, educational facilities, and other critical infrastructure rely on digital systems for daily operations. Government ministries in many countries use cloud computing services for data storage and processing that are provided primarily by US companies. Banks and other financial firms depend on US-dominated payment networks and data centers. Telecommunications networks route through infrastructure controlled mostly by US entities. This digital architecture, while necessary for fueling economic growth and administrative efficiency, has created significant strategic vulnerabilities.

The US government has increasingly weaponized non-military systems and used them as tools to serve its geopolitical interests.[1] Scholars have focused extensively on the weaponization of the international financial system, which is based on the dollar as the global reserve currency.[2] The United States has imposed unilateral coercive measures, commonly known as sanctions, on dozens of countries. This has led to a fragmentation of the financial system and a gradual move toward dedollarization, as sanctioned states like Russia build alternative institutions.[3]

There has also been extensive research on the vulnerabilities posed by the supply chain for critical minerals.[4] Nations are often left dependent on a single country, such as China, which processes the majority of many critical minerals. The trade war launched by the United States against China in 2018 illustrated how this can be a strategic vulnerability, as China restricted the export of rare earth elements in response to unilateral US tariffs.

Little academic research has, however, been published on Washington's weaponization of digital dependencies, despite the fact that many foreign countries rely on digital infrastructure provided by US technology firms.

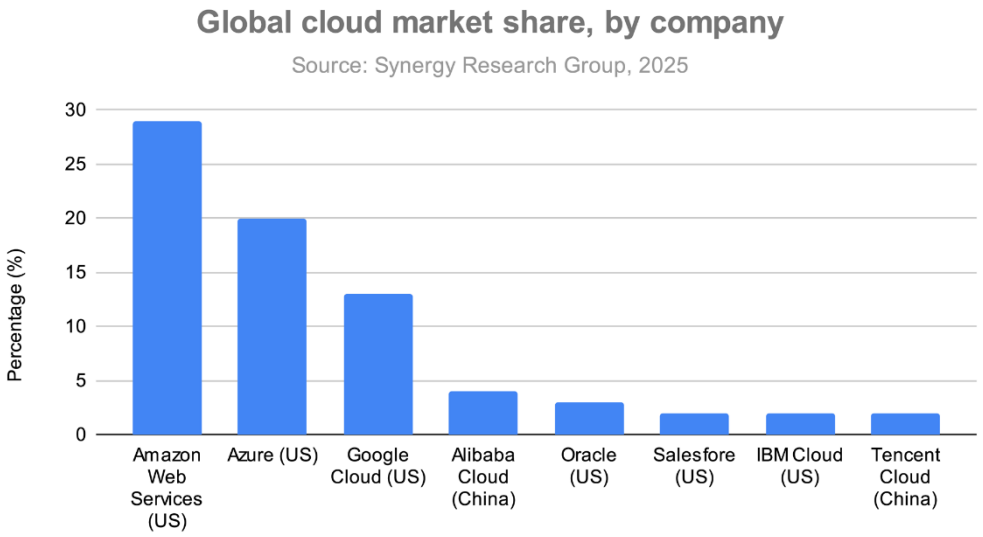
The concept of digital sovereignty is relatively new in Western discourse. In the 2010s, the term was used primarily by the Chinese government, which has long recognized how US technology firms could be used to advance Washington's political interests and interfere in the internal affairs of foreign nations.[5] As great power competition has intensified, some Western countries have made digital

[1] Nicholas Mulder, *The Economic Weapon: The Rise of Sanctions as a Tool of Modern War*, Yale University Press, 2024.
[2] Edward Fishman, *Chokepoints: American Power in the Age of Economic Warfare*, Penguin Random House, 2025.
[3] Daniel McDowell, *Bucking the Buck: US Financial Sanctions and the International Backlash against the Dollar*, Oxford University Press, 2023 and Agathe Demarais, *Backfire: How Sanctions Reshape the World Against U.S. Interests*, Columbia University Press, 2024.
[4] International Energy Agency (IEA). *Energy Technology Perspectives 2023*. https://www.iea.org/reports/energy-technology-perspectives-2023
[5] Jiang Min, "Models of State Digital Sovereignty from the Global South: Diverging Experiences from China, India and South Africa", *Policy & Internet*, Volume 16, Issue 4, December 2024 and Liao Fan, "Digital Sovereignty and Global Digital Governance", Jinan Journal, Volume 46, Issue 7, 2024.

sovereignty a priority. In 2021, the heads of state of Germany, Denmark, Estonia, and Finland issued a call for a digital sovereignty initiative in Europe. The World Economic Forum even published a policy paper on digital sovereignty in 2025.[6]

The present article focuses specifically on the problems faced by small states in the Global South, with an emphasis on Latin America. Their national security concerns vis-à-vis technology have become particularly acute, amid heated US-China rivalry. Brazil's President Luiz Inácio Lula da Silva, in particular, has criticized US Big Tech corporations, accusing them of meddling in his country's internal affairs and violating its sovereignty.[7]

Most countries on Earth are extremely dependent on US digital infrastructure. Just three US "hyperscaler" companies control 62% of the global market for cloud computing infrastructure: Amazon Web Services (AWS) has a 29% market share, Microsoft's Azure has 20%, and Google Cloud has 13%, as of the third fiscal quarter of 2025 (Figure 1).[8]



The world saw a clear example of how overreliance on firms from a single country can cause serious economic harm and political instability in October 2025, when there were global blackouts of cloud services provided by both AWS and Azure. Forbes magazine described this as a "wake-up call" that "raises questions" for the world.[9] British state media platform the BBC asked, "Are we relying too much

---

[6] Sean Fleming, "What is digital sovereignty and how are countries approaching it?", World Economic Forum, 10 January 2025, https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/

[7] EFE, "Lula afirma que las 'big tech' de EE.UU. deberán respetar las leyes brasileñas", 26 August 2025, https://es-us.noticias.yahoo.com/lula-afirma-big-tech-ee-135801242.html

[8] Synergy Research Group, via Statista, "Cloud Market Share Trends - Big Three Together Hold 63% while Oracle and the Neoclouds Inch Higher", 19 November 2025, https://www.srgresearch.com/articles/cloud-market-share-trends-big-three-together-hold-63-while-oracle-and-the-neoclouds-inch-higher

[9] Sanjit Singh Dang, "AWS And Azure Failures Raise Questions About Cloud Reliability", Forbes, 27 November 2025, https://www.forbes.com/sites/sanjitsinghdang/2025/11/27/aws-and-azure-failures-raise-questions-about-cloud-reliability/

on US big tech?"[10]

While those incidents were unintentional technical failures, they caused significant disruption across multiple countries, and illustrated how concentrated control over digital infrastructure creates systemic risk. Service interruptions affected government operations, obstructed financial transactions, and disrupted essential services, including healthcare systems. At least a dozen medical sites used by the UK's National Health Service (NHS), for instance, were impacted by the AWS outage.[11]

This is not just a hypothetical concern. In 2024, the International Criminal Court (ICC) issued an arrest warrant for Israel's Prime Minister Benjamin Netanyahu and Defense Minister Yoav Gallant, charging them with having committed war crimes and crimes against humanity against the Palestinian people in Gaza. In response, the US government imposed sanctions on ICC officials in 2025. This led ICC staff, including the chief prosecutor of the court, Karim Khan, to lose access to their official email accounts, which were provided by Microsoft.[12]

Similarly, the US government imposed unilateral sanctions against the sitting president of Colombia, Gustavo Petro, as well as the United Nations special rapporteur on the situation of human rights in the Palestinian territories occupied since 1967, Francesca Albanese. This meant that these prominent public figures cannot use services provided by US technology companies, and were blocked from accessing their bank accounts and from working with universities.[13]

Many US firms have likewise ceased operations in countries due to sanctions imposed by Washington, such as China, Russia, and Iran.[14] As the United States weaponizes the financial system, trade arrangements, and supply chains, it is likely that it will also increasingly use its dominance of digital technologies as a tool to serve its political interests.

In Latin America in particular, public and private institutions rely overwhelmingly on US cloud infrastructure.[15] This is a region that has also long suffered from US interventions. Researchers at the Congressional Research Service found that the US military has carried out operations in nearly all of the

---

[10] Liv McMahon, "AWS outage: Are we relying too much on US big tech?", BBC, 22 October 2025, https://www.bbc.com/news/articles/c0jdgp6n45po

[11] Jordan Sollof, "AWS outage causes disruption to patient care across NHS sites Cyber Security", Digital Health, 21 October 2025, https://www.digitalhealth.net/2025/10/aws-outage-causes-disruption-to-patient-care-across-nhs-sites/

[12] Molly Quell, "Trump's sanctions on ICC prosecutor have halted tribunal's work", Associated Press, 15 May 2025, https://apnews.com/article/icc-trump-sanctions-karim-khan-court-a4b4c02751ab84c09718b1b95cbd5db3

[13] El Heraldo, "Cuentas bancarias del presidente Petro, su familia y del ministro Benedetti serán congeladas por decisión de EE. UU.", 25 October 2025, https://www.elheraldo.co/colombia/2025/10/24/cuentas-bancarias-del-presidente-petro-su-familia-y-del-ministro-benedetti-seran-congeladas-por-decision-de-ee-uu/; and Gabriele Barbati, "UN rapporteur Albanese's family sues US officials over sanctions", 27 February 2026, Euronews, https://www.euronews.com/2026/02/27/un-rapporteur-albaneses-family-sues-us-officials-over-sanctions

[14] Yale School of Management, "Over 1,000 Companies Have Curtailed Operations in Russia—But Some Remain", 28 January 2024, https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain

[15] Cecilia Rikap, "South America's sovereignty is being lost in Big Tech's clouds", OpenDemocracy, 30 July 2025, https://www.opendemocracy.net/en/south-america-big-tech-brazil-chile-data-centres-united-states/

countries in Latin America.[16] In January 2026, the US military bombed Venezuela, invaded its territory, and abducted its internationally recognized President Nicolás Maduro. Just a few weeks later, in February, the US military imposed a naval blockade on Cuba, preventing the country from importing oil in an attempt to collapse its economy and overthrow its government.

If Washington decided to intentionally weaponize the digital infrastructure provided by US tech companies by cutting off a Latin American nation's access to cloud services, it could cause severe instability.

Geopolitical dimensions of digital infrastructure, and resource limitations

The strategic importance of digital infrastructure extends beyond technical considerations. This is not just a hypothetical fear. The United States has already demonstrated willingness to use digital systems as instruments of foreign policy. The New York Times reported that the US government launched cyber-attacks on Russia's power grid.[17] Washington has reportedly infiltrated Russian electrical infrastructure since at least 2012, inserting what the Times called "crippling malware". The newspaper described this operation as part of a "digital Cold War". Moreover, the United States and Israel developed the Stuxnet virus in order to destroy Iran's nuclear infrastructure.[18] Then, in February 2026, Washington and Tel Aviv launched a war against Tehran, and President Donald Trump publicly threatened to destroy Iran's electrical infrastructure.[19]

It is becoming clear that digital infrastructure is a sector that will be weaponized in the wars of the 21st century. This makes it extremely important for states to formulate policies to preserve their digital sovereignty and security, before it is too late.

For small countries in the Global South that have limited domestic technology sectors, this reality creates a fundamental policy dilemma. Dependency on foreign technology providers – especially those headquartered in the United States, which has a long history of intervening in foreign countries and violating their sovereignty – exposes national systems to potential disruption. In particular, Latin America's historical experience with foreign intervention compounds these concerns and necessitates

[16] Barbara Salazar and Sofia Plagakis, "Instances of Use of United States Armed Forces Abroad, 1798-2023", US Congressional Research Service, 7 June 2023, https://sgp.fas.org/crs/natsec/R42738.pdf
[17] David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid", New York Times, 15 June 2019, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html
[18] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran", 1 June 2012, New York Times, https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html
[19] Lim Hui Jie and Victor Loh, "Trump threatens to destroy Iranian infrastructure, saying its government 'knows what has to be done'", 3 April 2026, CNBC, https://www.cnbc.com/2026/04/03/trump-iran-threats-un-resolution-blocked-strait-of-hormuz-f35-shot-down.html

careful consideration of technology sourcing decisions. Unlike large economies capable of developing comprehensive domestic technology ecosystems, most developing countries face resource constraints that make technological self-sufficiency impossible. They lack the size, capital, technical workforce, and market scale necessary to replicate the innovation capacity of major technology powers. This reality requires strategies that acknowledge these limitations while still reducing vulnerability and preserving sovereign decision-making over critical systems.

Evaluating technology partnership options

The current landscape of technology partnerships presents trade-offs requiring careful assessment. Continued reliance on US providers maintains current operational continuity but perpetuates dependency relationships with associated vulnerabilities. Alternative partnership configurations offer potential benefits but introduce their own considerations.

Option A: Diversification through alternative partnerships

Latin America can consider engaging alternative technology providers, especially those from nations without histories of unilateral intervention in the region. Principal among the options is China. China has a proven track record of respecting the sovereignty of Latin American nations and refraining from meddling in their internal affairs. East Asia is far away from the region, and thus far Beijing has shown respect for Latin American nations' sovereignty – certainly much more so than the United States, which has constantly intervened in Latin America and has invaded most of the countries in the region.

In their foreign policy, some Latin American states have sought to lean closer to China as a counterbalance against the United States. This was apparent in Cuba, Nicaragua, Venezuela, Brazil under the Workers' Party, Argentina under the left-wing Peronists, Bolivia under President Evo Morales, Honduras under the Libre Party, and Ecuador under President Rafael Correa. Countries should consider the same kind of diversification in the technological realm. Chinese technology firms offer mature cloud computing platforms, telecommunications infrastructure, and digital payment systems that could serve as alternatives or complements to US providers. Moreover, Chinese firms tend to provide services at a lower price point than their US competitors.[20] This could therefore help reduce government outlays, and soften the financial burden on private companies, which also need such infrastructure.

This option is not only realistic; it could be implemented immediately, given that Chinese firms already have the technological infrastructure necessary to at least diversify reliance on US technology, if not

[20] US-China Business Council, "Competition with Chinese Firms Tops Challenges for American Companies in China", 26 September 2014, https://www.uschina.org/articles/competition-with-chinese-firms-tops-challenges-for-american-companies-in-china/

replace it. However, this strategy requires careful implementation. Simply substituting one dependency for another would not guarantee digital sovereignty. To date, China has not aggressively interfered in Latin America's internal affairs, and in the short to medium term this does not seem likely. However, if there are unforeseen changes in the future, Beijing could also potentially weaponize the region's dependency on Chinese technology, just as Washington has demonstrated a willingness to weaponize foreign nations' dependency on US technology. Nevertheless, this hypothetical future concern pales in comparison to the tangible present threat posed by belligerent US policy.

Implementation of alternative technology infrastructure requires substantial capital investment. Development financing from international sources offers a potential mechanism for funding these initiatives. Many Global South states are members of the Belt and Road Initiative (BRI), and Chinese policy banks have provided infrastructure financing to many developing countries at concessional rates, often with flexible repayment terms suited to countries with limited fiscal space. However, financial arrangements warrant careful evaluation. All external financing creates obligations that must be weighed against benefits. Terms should be transparent, sustainable relative to government revenues, and structured to avoid creating new dependencies that undermine sovereignty objectives.

Option B: Regional cooperation framework

Another option could be to coordinate with neighboring nations to develop shared technological infrastructure. This offers the potential for building capacity that exceeds what any individual small country could achieve. Regional cooperation could enable joint investment in data centers, shared development of certain technological capabilities, and collective bargaining power when negotiating with technology providers. This approach aligns with broader regional integration objectives and creates opportunities for South-South cooperation. It requires sustained diplomatic coordination, harmonization of technical standards, and mechanisms for equitable cost-sharing among participating nations with varying economic capacities.

This option does present its own series of problems. Not all regions have the scale, capital, and technical expertise necessary to implement such a proposal. The ASEAN nations in Southeast Asia, to take one case, are much more integrated than the states of the African Union or the members of the Community of Latin America and Caribbean States (CELAC).[21] Even within regions, there are contradictions. In Latin America, Brazilian and Mexican firms may offer some flexibility and reduce technological dependency, but their sophistication and quality is still significantly lower than that of Chinese firms.

The United States and China are the only two countries that have companies with the most advanced

[21] Felipe Larraín B. and Carmen Cifuentes V., "To Rethink Latin American Integration, Look to ASEAN", 23 June 2025, Americas Quarterly, https://americasquarterly.org/article/to-rethink-latin-american-integration-look-to-asean/

technologies. A look at the global cloud computing market, for instance, shows it is dominated by US and Chinese companies. For cloud computing, Chinese firms may be a more realistic option. But for servers, hosting providers, and telecommunications equipment, there are companies in Latin America that can offer some of these services. This option, therefore, is something to consider in the medium to the long term. If Latin American states can work together to promote digital sovereignty, it is possible to develop these capacities in the upcoming decade or two. But it would be difficult to transition in the short term.

Regardless of which technology providers are engaged, reducing dependency further requires developing domestic technical expertise. Current gaps in the technology workforce in many developing countries limit their ability to operate, maintain, and make informed decisions about complex digital systems. Without strengthening domestic capacity, technology partnerships will necessarily remain dependent relationships regardless of which foreign partners are involved.

Building technical capacity requires sustained government investment in education, training programs for IT personnel, and the cultivation of career pathways that retain skilled professionals in public service. This represents a multi-year commitment, but it is essential for any meaningful sovereignty enhancement. It would also generate positive externalities for the economy, promoting higher rates of growth and formal employment.

Option C: Status quo maintenance

Maintaining current technological dependence on US firms would be the easiest option, with the lowest cost, as countries would not have to transition to any new infrastructure. However, this approach leaves fundamental vulnerabilities unaddressed and fails to reduce exposure to external disruptions. The October 2025 blackout incidents demonstrated that even unintentional failures can cause significant harm under current arrangements. Moreover, the Donald Trump administration's attacks against Venezuela, Iran, and Cuba, as well as threats to impose high tariffs on many countries, suggest an intensification of US pressure in the near future, so protecting digital sovereignty must be a priority in the short term.

The following table (Figure 2) outlines potential options:

Digital sovereignty proposals

Option A: Diversification through alternative partnerships Engage alternative providers, primarily Chinese technology firms	• Reduces dependencies on the US • Engages providers from China, which does not have a history of interventionism in Latin America • Chinese firms offer competitive, lower cost platforms, for cloud computing, telecoms, and payments	• Risk of substituting one dependency for another • Significant transition costs and technical migration challenges • Requires retraining workers on new platforms and systems • Potential interoperability issues

	• Decreases US leverage over Latin America • Access to concessional financing through Chinese policy banks • Creates competitive pressure that may improve terms with all providers	between different technology ecosystems • Need for careful evaluation of new providers' security practices • Financing arrangements require scrutiny to ensure sustainable terms
Option B: Regional cooperation framework Coordinate with Latin American partners to develop shared infrastructure	• Pools resources beyond what individual small countries can achieve • Enables joint data centers and shared technological capabilities • Creates collective bargaining power with technology providers • Aligns with broader regional integration objectives • Facilitates South-South cooperation and knowledge sharing • Distributes infrastructure across multiple countries, reducing single points of failure • Builds regional technical capacity and expertise	• Requires sustained diplomatic coordination across multiple governments • Necessitates harmonization of technical standards and regulatory frameworks • Complex mechanisms needed for equitable cost-sharing among countries with varying capacities • Slower decision-making due to need for multi-country consensus • Success depends on continued commitment from partner nations • Requires significant upfront investment before benefits materialize
Option C: Status quo maintenance Continue current reliance on existing US technology providers	• Operational continuity with minimal disruption • Established vendor relationships • No immediate transition costs	• Perpetuates strategic vulnerabilities to external disruption • Maintains dependency on providers from the US, with a history of aggressive interventionism • Leaves infrastructure exposed to potential weaponization • October 2025 blackout incidents demonstrated fragility of concentrated dependencies • Fails to address underlying sovereignty concerns

Policy Recommendations

Based on the analysis above, this article recommends a phased, multi-component strategy that balances near-term operational needs with long-term sovereignty objectives.

Recommendation 1: Implement gradual technology diversification

States should establish a Technology Diversification Working Group within national ministries or institutes of technology, with representatives from relevant ministries, institutes, regulatory agencies, and technical experts.

This process can be implemented gradually, in phases. Governments can start by transitioning state institutions that rely on cloud computing services provided by US firms (such as AWS, Azure, Google Cloud, and Oracle), and instead sign contracts with Chinese competitors like Alibaba Cloud and Tencent Cloud. After public institutions have transitioned, state authorities can encourage private enterprises to do the same, by offering incentives like small tax breaks and technical assistance.

This working group should conduct a comprehensive audit of current digital infrastructure dependencies, mapping which systems rely on which US providers and identifying critical single points of failure. It should then develop a prioritization framework that identifies which systems should be diversified first, based on strategic importance. It should then create a phased migration plan that gradually introduces alternative providers for non-critical systems initially, building experience before transitioning to more sensitive infrastructure.

Recommendation 2: Strengthen regional technology cooperation

Global South countries should pursue bilateral and multilateral technology cooperation agreements with neighboring countries through existing regional mechanisms.

For Latin America, specific actions include proposing a Digital Infrastructure Initiative within the Community of Latin American and Caribbean States (CELAC) and sub-regional bodies like the Union of South American Nations (UNASUR) and Central American Integration System (SICA). States in the region could also negotiate bilateral agreements with friendly countries outside of Latin America, like China, Russia, Iran, Vietnam, and South Africa, which share similar concerns about digital sovereignty.

Recommendation 3: Develop domestic technical capacity

Launch a National Digital Sovereignty Capacity Building Program that focuses on expanding computer science and cybersecurity programs at national universities, with generous stipends for students who commit to public sector service upon graduation. The government could also establish a program that recruits technology professionals into government roles, offering competitive salaries and professional development opportunities.

Recommendation 4: Establish a governance framework for technology sovereignty

Create formal institutional structures and policies that embed sovereignty considerations in technology decision-making. This could include enacting a Digital Sovereignty Act that establishes a legal framework for technology procurement decisions, data localization requirements for sensitive government information, and security standards for critical infrastructure. States could also establish a National Digital

Sovereignty Council, with membership from relevant ministries, that reviews major technology procurement decisions and strategic technology partnerships.

Conclusion

Digital sovereignty represents a complex policy challenge for small countries. Complete technological independence is not possible. However, current dependency arrangements on US firms create unacceptable vulnerabilities that compromise national security and sovereign decision-making. The recommended strategy acknowledges these constraints while charting a pragmatic path forward. The geopolitical environment makes these efforts urgent. US intervention in the internal affairs of Latin American countries is likely to increase in the near future, especially as US-China tensions grow. Digital infrastructure has become a domain of strategic competition, and countries that fail to address vulnerabilities will find their sovereignty increasingly constrained. Small states have the imperative to act decisively in protecting their digital future.

Bibliography

[1] Barbati, Gabriele. "UN rapporteur Albanese's family sues US officials over sanctions". 27 February 2026. Euronews. https://www.euronews.com/2026/02/27/un-rapporteur-albaneses-family-sues-us-officials-over-sanctions

[2] Dang, Sanjit Singh. "AWS And Azure Failures Raise Questions About Cloud Reliability". Forbes. 27 November 2025. https://www.forbes.com/sites/sanjitsinghdang/2025/11/27/aws-and-azure-failures-raise-questions-about-cloud-reliability/

[3] Demarais, Agathe. *Backfire: How Sanctions Reshape the World Against U.S. Interests*. Columbia University Press. 2024.

[4] EFE, "Lula afirma que las 'big tech' de EE.UU. deberán respetar las leyes brasileñas", 26 August 2025, https://es-us.noticias.yahoo.com/lula-afirma-big-tech-ee-135801242.html

[5] El Heraldo. "Cuentas bancarias del presidente Petro, su familia y del ministro Benedetti serán congeladas por decisión de EE. UU.". 25 October 2025. https://www.elheraldo.co/colombia/2025/10/24/cuentas-bancarias-del-presidente-petro-su-familia-y-del-ministro-benedetti-seran-congeladas-por-decision-de-ee-uu/

[6] Fishman, Edward. *Chokepoints: American Power in the Age of Economic Warfare*. Penguin Random House. 2025.

[7] Fleming, Sean. "What is digital sovereignty and how are countries approaching it?". World Economic Forum. 10 January 2025. https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/

[8] International Energy Agency (IEA). *Energy Technology Perspectives 2023*. https://www.iea.org/reports/energy-technology-perspectives-2023

[9] Jiang Min. "Models of State Digital Sovereignty from the Global South: Diverging Experiences from China, India and South Africa", *Policy & Internet*, Volume 16, Issue 4, December 2024, pp. 727-738.

[10] Jie, Lim Hui and Victor Loh. "Trump threatens to destroy Iranian infrastructure, saying its government 'knows what has to be done'". 3 April 2026. CNBC. https://www.cnbc.com/2026/04/03/trump-iran-threats-un-resolution-blocked-strait-of-hormuz-f35-shot-down.html

[11] Larraín B. Felipe and Carmen Cifuentes V. "To Rethink Latin American Integration, Look to ASEAN". 23 June 2025. Americas Quarterly. https://americasquarterly.org/article/to-rethink-latin-american-integration-look-to-asean/

[12] Liao Fan, "Digital Sovereignty and Global Digital Governance", Jinan Journal, Volume 46, Issue 7, 2024, pp. 47-60.

[13] McDowell, Daniel. *Bucking the Buck: US Financial Sanctions and the International Backlash against the Dollar*. Oxford University Press. 2023.

[14] McMahon, Liv. "AWS outage: Are we relying too much on US big tech?". BBC. 22

October 2025. https://www.bbc.com/news/articles/c0jdgp6n45po

[15] Mulder, Nicholas. *The Economic Weapon: The Rise of Sanctions as a Tool of Modern War*. Yale University Press. 2024.

[16] Quell, Molly. "Trump's sanctions on ICC prosecutor have halted tribunal's work". Associated Press. 15 May 2025. https://apnews.com/article/icc-trump-sanctions-karim-khan-court-a4b4c02751ab84c09718b1b95cbd5db3

[17] Salazar, Barbara and Sofia Plagakis. "Instances of Use of United States Armed Forces Abroad, 1798-2023". US Congressional Research Service. 7 June 2023. https://sgp.fas.org/crs/natsec/R42738.pdf

[18] Sanger, David E. "Obama Order Sped Up Wave of Cyberattacks Against Iran". 1 June 2012. New York Times. https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

[19] Sanger, David E. and Nicole Perlroth. "U.S. Escalates Online Attacks on Russia's Power Grid". New York Times. 15 June 2019. https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

[20] Sollof, Jordan. "AWS outage causes disruption to patient care across NHS sites Cyber Security". Digital Health. 21 October 2025. https://www.digitalhealth.net/2025/10/aws-outage-causes-disruption-to-patient-care-across-nhs-sites/

[21] Synergy Research Group. "Cloud Market Share Trends - Big Three Together Hold 63% while Oracle and the Neoclouds Inch Higher". 19 November 2025. https://www.srgresearch.com/articles/cloud-market-share-trends-big-three-together-hold-63-while-oracle-and-the-neoclouds-inch-higher

[22] US-China Business Council. "Competition with Chinese Firms Tops Challenges for American Companies in China". 26 September 2014. https://www.uschina.org/articles/competition-with-chinese-firms-tops-challenges-for-american-companies-in-china/

[23] Yale School of Management. "Over 1,000 Companies Have Curtailed Operations in Russia—But Some Remain". 28 January 2024. https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain