

# Cloud Computing in Southeast Asia and Digital Competition with China

By James A. Lewis

---

The world is building the global digital infrastructure that connects people and countries. This is not the traditional physical infrastructure of roads or bridges but a massive, interconnected enterprise composed of undersea cables, fiber-optic networks, telecommunications, satellites, software, and cloud computing services. Billions of dollars are being spent to build the global digital infrastructure since digitization is the key to economic growth.

Digitization requires cloud computing. Cloud technology is digitization's infrastructure. Cloud computing and services are the data and computing backbone of digital economies. They have become a focal point for international tech competition. Decisions that countries and companies make about which cloud providers to use will shape the future of commerce, global influence, and international security.

Identifying the central role of communications technology in international affairs is not new. The first generation of geopolitical scholars, writing more than a century ago, saw telecommunications (telecom) and global connectivity as an essential aspect of national power. Today, over 100 years later, digital connectivity plays a much larger role in shaping national power and influence. We can extend these early geopolitical concepts to say that whoever provides the world's digital communications infrastructure and service will reshape international affairs.

The use of cloud technologies raises difficult policy issues for national security and technology policy. This report on cloud competition in Southeast Asia is a companion piece to others in a **series** from the Center for Strategic and International Studies (CSIS). The series includes reports on cloud competition that examine the strategic implications of competition for the global political environment and highlight the need to use trustworthy cloud service providers (CSPs). This report makes recommendations for how the United States can best protect the interests of democracies in the new competition over cloud infrastructure.

The Global South is the primary arena for competition when it comes to cloud computing. This report looks at Southeast Asia, a strategically crucial region and one of the most economically dynamic regions in the world (see a separate **CSIS report** for a discussion of cloud competition in Latin America). The United States has an opportunity to shape national decisions on cloud infrastructures in Southeast Asia to advance its larger digital agenda of establishing economic opportunity and trustworthy technologies. Success in Southeast Asia would help promote democracy and the rule of law, create economic opportunity for Western companies and regional participants, and set precedents for policy in other regions.

The competitor in this is, of course, China. Competition is both commercial and strategic. Many believe that China has a strategy to gain global economic dominance and advance its **centralized and undemocratic system of governance**. China supports its companies to gain market share as part of a larger effort to increase political influence. The United States does not provide similar support to its firms, and though U.S. cloud companies offer better technology and services, a failure to create a supportive political framework in the United States will create opportunities for China and risks to U.S. interests.

## RECOMMENDATIONS

- Create a comprehensive approach that emphasizes economic growth.
- Emphasize the importance of trustworthy networks and cloud services.
- Work with Japan and Australia to make the case for trust.
- Commit to privacy and data protection by extending transatlantic agreements.
- Streamline foreign assistance processes and make cloud and connectivity a top priority.
- Expand workforce training and assistance, particularly cybersecurity training.
- Link trustworthy cloud computing to sustainability.
- Highlight for regional audiences the importance of a trustworthy cloud for broader security relationships with the United States.
- Reconsider domestic antitrust initiatives that may weaken U.S. companies.
- Demonstrate a commitment to improve trade ties with the region.

### *What Is the Cloud?*

An earlier CSIS report, “**An Overview of Global Cloud Competition**,” describes the strategic importance of cloud computing. The term “the cloud” describes the provision of services to provide infrastructure, software, computing power and data storage. There are public clouds, provided by vendors (the largest are known as “hyperscalers” because of their massive size); private clouds, where a company or agency operates its own cloud; and hybrid clouds, where companies use a mix of public and private clouds. “Multicloud” refers to buying services from more than one provider.

The cloud is created by interconnected networks of data centers (facilities that houses large numbers of computers connected to each other and to the internet), where companies and governments store and

process data. For public clouds (where software tools, computing, and memory resources are provided by a third party), data and connections are managed by a CSP. If someone uses one of the popular email services like Outlook or Gmail, they are using the cloud. Cloud competition is about who provides these infrastructures and services and under what conditions.

Cloud services offer resilience, lower costs, and better security. Equally important, they are a foundational technology for innovation. This makes them a powerful tool for growth and development. Cloud services provide economic and security advantages, but they can also create dependencies on the infrastructure and service providers that have broad strategic implications.

Cloud services are an essential component of the networks that make up the internet and telecom services. Starting with 5G, future generations of telecom networks will depend even more on the cloud. This reliance on cloud services reinforces their strategic importance. Owning or operating the cloud is a strategic function because it gives a degree of control over data and services and can create potential risks for espionage and disruption. This makes trust a central issue for policy—determining if the CSP is trustworthy, the same way the issue of trust was central to the discussion of 5G.

### *Why Cloud Services Are Strategic*

In a long-lasting contest where both sides may prefer to avoid the direct use of force, technology and information have become more important in creating national power and shaping international relations. Cloud services have become a strategic issue because digitization has reshaped the contours of international competition and has created new kinds of international influence and strength. Cloud services create dependencies that are easy to exploit if the provider or its government are not trustworthy.

U.S. policy cannot be based on blocking China if it is to attract support. The goal is to ensure that the emerging global structure of fiber-optic cables, satellites, next generation telecom, and the cloud will promote development, enhance trust and security, and guarantee that the policies governing this global structure are transparent, fair, and based on the rule of law. This makes setting the rules for cloud competition, in cooperation with like-minded nations—as was done for 5G infrastructure—a central task for U.S. foreign policy.

Cloud policy must balance the opportunities for development and growth against the potential risks. The potential risks from cloud computing fall into several categories. There is the security of the data stored on the cloud, where the risk will be determined by how that data is stored, encrypted, and managed. There is also a risk to sovereignty and privacy if data is stored outside national borders without appropriate safeguards. And cloud services play an increasingly important role in cybersecurity. Cloud services from an untrustworthy provider create risks to security and sovereignty and creates the potential for coercion, espionage) or for the disruption of data and services. A failure to make full use of the cloud will also damage national security by reducing economic growth and innovation—the “opportunity cost” of lost income and invention. One major risk is not immediately apparent. Supplying and operating the cloud makes it likely that customers will use other technology built to the supplier’s standards, creating a kind of “vendor dependency” for years to come.

The choice of CSP can establish dependency on suppliers not just for the cloud, but also for the digital

technologies that use the cloud. Chief among these are telecom and financial networks, but there is also a large and growing set of devices like robots or autonomous cars. Phones and networks will not work without access to the cloud, airlines and banks rely on the cloud, and soon cars and factories will be similarly dependent. This makes who operates the cloud, and under what rules and conditions, an essential question for security.

## *Cloud Competition in Southeast Asia*

Southeast Asia is one of the regions where digital competition is most intense. The region **leads the world** as a market for **cloud computing**. This makes it a market where any large CSP will want to compete. It is a politically diverse region with democracies, communist states, military juntas, and dictatorships, as well as a few governments that have been labeled “authoritarian.” Its countries range from giant Indonesia to tiny (and economically powerful) Singapore. It is strategically important given its location and economic dynamism and is growing at an unmatched rate. Data from the International Monetary Fund (IMF) show Southeast Asia’s aggregate income as close to \$4 trillion. Some countries like Myanmar are among the poorest in the world, while others like Singapore are among the wealthiest. Many of the countries in the region have a strong entrepreneurial culture (for example in FinTech and e-commerce, which are dependent on cloud services). Innovation and entrepreneurship create demand for cloud services. U.S. and Chinese cloud giants compete for this important regional market. The terms of competition are fundamentally economic and commercial, more about development than security.

Development and sovereignty are the primary drivers of national cloud policies in the region. The emphasis given to these topics can vary from country to country, but U.S. policy needs to be able to address both in terms that appeal to other nations. This means that for some audiences in Southeast Asia, an appeal that only highlights the national security risks created by China’s behavior, without highlighting the economic opportunities, will be unpersuasive. This dynamic has been played out in other regions, including Latin America.

Southeast Asian officials sometimes describe their situation as a mouse caught between two sparring elephants. Most countries in the region have long-standing connections to China. A few countries, such as Laos and Cambodia, are firmly in the Chinese camp. Other Southeast Asian countries prefer to balance relations with the two competitors. There can be distrust of China that the more distant United States does not face. Malaysia, Indonesia, and Vietnam have a history of suspicion regarding China’s regional pretensions. China’s territorial aggrandizements challenge the Philippines.

This is a complex political landscape. The growth of cloud computing in Southeast Asia is driven by the region’s digital transformation, favorable government policies, and increased demand for information technology infrastructure and infrastructure modernization. Growth in demand for cloud services is also driven by the rise in the number of digital tech start-ups in the region, led by Singapore, Indonesia, Thailand, and the Philippines. U.S. cloud companies have a leading market share, but Chinese companies intend to displace them, so the United States needs to make the case for trustworthy cloud infrastructure and services.

## *Data Localization and Data Sovereignty*

Data localization, where countries require their citizens' data to be stored in their territory, is a global phenomenon—a reaction to U.S.-led globalization that first shaped the internet. Data governance has become a concern for policymakers as they grasp data's value and as they seek to reassert sovereign control over what they see as a national resource. These efforts are often linked to privacy and data protection concerns, and localization can improve performance for users by reducing latency (the time between a client's request and an answer). In general, these requirements are not the most economic approach to cloud services, but data localization **can negate** the efficiencies cloud services can offer, as rules are not harmonized among nations and as restrictions on data transfers harm business. Data localization can also lead to less resiliency, result in less access to leading edge cloud services, and reduce innovation.

Contrary to the hopes of many governments, data localization does not improve security. In fact, it can weaken it. Data security is provided by encryption and cyber hygiene to secure networks and by ensuring contracts with service providers offer protection. However, these arguments are often irrelevant to the political and legal concerns that drive localization. What data localization provides to national governments is greater trust and control. Localization makes data (or the physical infrastructure that contains it) subject to national jurisdiction.

The central issue for localization is the extraterritorial storage of data. The internet provides almost instantaneous connectivity regardless of borders, and cloud technologies can store and process immense quantities of data irrespective of location. The use of this data creates immense business opportunities but also challenges national sovereignty, since the application of national laws is bounded by national borders. The conventional location-based approach to law and regulation is inadequate. Countries have not agreed on how to govern the global digital environment, but many are drawn to increased national regulation.

Data localization laws usually seek to ensure that data created or acquired within a country is stored, processed, and sometimes used in that country. A few years ago, relatively few countries around the world had data localization regulations. Now, more than half of all nations have some form of data localization rules. Countries see localization rules as a tool to provide “data sovereignty,” using requirements and limitations for cross-border data flows. Localization does not improve security, but data localization requirements can allow local law enforcement access to nationally stored data and, at least in Europe, prevent the perceived risk of the U.S. government accessing the data. The dilemma is that these restrictions can damage growth and even security, as when Ukraine had to hurriedly revise its data localization laws to allow it to move essential data outside the reach of Russian attacks.

In Southeast Asia, Malaysia, **Indonesia, and Vietnam** have data localization laws. Restrictions on the cross-border flow of data limits the transfer of important information—like financial or medical records. This forces companies to build **additional storage capacity** in country. Association of Southeast Asian Nations (ASEAN) governments say there are three reasons behind localization **requirements**: (a) it is easier for national law enforcement agencies to access domestically stored data than data stored abroad, (b) they believe data localization offers better protection from cyberespionage, and (c) localization increases privacy protections.

Localization requirements are often presented as necessary for privacy. Singapore, Malaysia, and the Philippines all have laws to protect personal data. Thailand is the latest ASEAN country to enact data protection laws, with the parliament passing the **Personal Data Protection Act** in early 2019. Indonesia has been mulling over a general data protection law and has drafted legislation. The remaining ASEAN countries do not have regulatory frameworks for data protection, but some have laws for specific sectors (like finance or health) that regulate personal data transfers.

ASEAN has taken an approach to data localization similar to that of the European Union, and some ASEAN countries are adapting **similar (but less stringent) policies** based on the European Union's General Data Protection Regulations (GDPR). Both regions have a strong interest in protecting the privacy of personal data if it is transferred or stored outside of the home country. One major difference, however, is that ASEAN as a region lacks the formal regulatory authority of the European Commission to administer these measures. ASEAN national are also more attuned to the potential economic consequences of overly stringent regulation.

One tension created by data localization requirements is that they can run counter to ASEAN countries' strong interest in the digitization of their economies, the growth of e-commerce, and the creation of a regionally integrated digital economy. Article 7 of the ASEAN Agreement on Electronic Commerce calls for member states to work toward "eliminating or minimizing barriers to the flow of information across borders," while taking into consideration "appropriate safeguards to ensure security and confidentiality of information." The same article also prohibits member states from demanding domestic computer facilities or data centers as a prerequisite for **in-country commerce**, providing signatory nations an ability to flexibly interpret their commitments. The agreement does not specifically mention cloud services, but its call to safely, securely, and confidentially improve cross-border information flow point to it,

Other provisions support improved **data governance** and ensuring responsible transborder data flows. The ASEAN Working Group on Digital Data Governance **adopted** voluntary Model Contractual Clauses for Cross Border Data Flows (ASEAN MCCs) in 2021, providing a template for extra-ASEAN data transfers. The emerging regulatory environment will shape the cloud services market and create opportunities for CSPs.

### *Cloud Service Providers in Southeast Asia*

The largest CSPs in Southeast Asia are U.S. and Chinese companies with globally recognized names. U.S. companies still have dominant market share in the region. Amazon Web Services (AWS), one of the leading CSPs globally, was an early entrant into the regional cloud market and has a major presence in Southeast Asia. Microsoft's Azure is second largest in the Southeast Asia cloud market. Both provide computing power, storage, databases, artificial intelligence (AI), and data analytics tools. Google Cloud Platform (GCP) is the third-largest U.S. supplier in the Southeast Asia region. IBM Cloud also has a strong presence in Southeast Asia given its offerings of both cloud services and hybrid cloud solutions. Together, AWS, Microsoft, and Google still hold the largest market share in ASEAN. Singapore and Indonesia are key countries for cloud competition because of their digitization and entrepreneurial tech environments, with companies like AWS, Huawei, and Alibaba planning to spend billions of dollars there.

U.S. cloud computing companies face rising competition from major Chinese rivals in Southeast Asia. As the domestic Chinese market becomes saturated and many European countries are reluctant to rely on Chinese service providers (given their links to the Chinese government), Chinese companies have turned to the developing world. The growing economies of Southeast Asia are especially attractive as China's domestic cloud market slows. Chinese companies offer lower-priced services and infrastructure, along with other benefits like workforce training, that are particularly attractive to developing economies. Chinese cloud companies offer low cost, scalable solutions. Chinese tech giants like Alibaba, Tencent, and Huawei are building data centers in Southeast Asia to serve the growing market and are **investing** hundreds of millions of dollars. Tencent and Huawei already claim to have more data centers in the region than AWS, Microsoft, or Google.

Tencent, with its large presence in gaming, e-commerce, and social media, currently has less market share than Amazon, Microsoft, Google, and Alibaba, but its strength in these other areas makes it a powerful competitor. Alibaba Cloud is the leading cloud provider in China, and it offers services that include AI capabilities. Huawei Cloud is part of Huawei's well-resourced global strategy to regain market dominance by supplying 6G and cloud services (and 6G will rely on the cloud). Some larger regional companies seek to increase resilience by using more than one CSP. The landscape **will change** as competition intensifies in the region. The issue for U.S. policy is not of a commercial nature, but rather in gaining regional acceptance and support for the need to build a trustworthy and secure global network.

Many ascribe a strategic intent to Chinese investments. Chinese companies argue that it is the natural pursuit of commercial advantage. **Both are probably true.** China has reportedly invested **\$500 billion in Southeast Asian countries**—mostly in transportation infrastructure that connects countries in the region to China—in the first five years of its Belt and Road Initiative (BRI), which is part of a larger effort to **increase its influence** and more closely tie other countries in the region to China, both economically and politically. This includes building tech supply chains that connect China and the region (to the detriment of the United States), increasing the use of the renminbi, and creating a China-centered network infrastructure.

The once-feared BRI has been slowed by **concerns** in recipient nations over debt and dependency, as well as by China's current economic difficulties. This creates an opportunity for the United States and its allies if they can show consistent support for infrastructure projects. The challenge for U.S. policymakers (and for Japanese and Australian allies) is how to make a compelling case for a digital infrastructure that is trustworthy and that counterbalances Chinese spending and economic support. The challenge goes beyond Southeast Asia. The country that builds this global infrastructure will gain and hold influence and technological leadership.

### *Recommendations for Promoting a Trustworthy Cloud Globally and in the Region*

At one level, cloud competition is over price and service, but there is an equally important political and diplomatic dimension that revolves around regional attitudes toward China. Although countries in the region want the United States to counterbalance China, it will remain an unavoidably important part of the region's political, business, and security landscape. This will shape the market for cloud services and infrastructure. The policies of countries in the region toward China will remain nuanced and

balanced. Pointing to the risk from China will not by itself change thinking on cloud suppliers.

While intelligence sharing can help make the case for concern over China's actions, arguments on the cloud and 5G that emphasize the risks of Chinese espionage or of doing business with a predatory trade partner will not be persuasive for an audience that is long-accustomed to China and its aspirations, and may have similar (if unspoken) concerns about the United States.

The goal for many countries in the region is, in varying degrees, to balance the two giants, to preserve both autonomy and access to two important markets. For the United States to compete, what is needed in Southeast Asia and other nations of the Global South is a comprehensive package of measures that emphasize economic development while also taking sovereignty concerns into account. The United States has advantages in this competition. Its technology is better, it has important allies, and ASEAN officials in many countries have a general preference for the rules-based international order centered on international law championed by the United States and its allies rather than the idiosyncratic China-centric alternative.

To capitalize on this, the United States must make a stronger case that a rules-based order is more likely to bring the economic development that is at the core of regional interests. The centerpiece of U.S. efforts must be a positive agenda for growth, and the United States needs to make the case in the global south that trustworthy cloud services create economic growth and are better for national sovereignty.

*For the United States to compete, what is needed in Southeast Asia and other nations of the Global South is a comprehensive package of measures that emphasize economic development while also taking sovereignty concerns into account.*

The United States, with Japan and Australia, can highlight how trust and secure data flows strengthen economies. Trustworthy cloud services and networks will better serve the vibrant start-up culture in Southeast Asia, allowing it to take advantage of the increased access to cloud services and the computing resources, data storage, and connectivity they provide. This can help businesses of all sizes be more competitive without taking on the risks that come from using untrustworthy providers. Trustworthy cloud will attract businesses and investors and is essential for emerging technologies like 5G, AI, the Internet of Things (IoT), and data analytics.

The United States and its allies can appeal to the regional desire to avoid dominance by China, emphasize the importance of security ties with the West, and point to the benefits of digital trust in suppliers. There is a need for a comprehensive approach. These recommendations identify the elements of a comprehensive approach and suggest how the United States can shape the cloud market in Southeast Asia and elsewhere. The United States can shape competition in ways that are helpful to both its companies and Southeast Asian countries by emphasizing a positive agenda that accelerates economic development. The following paragraphs sketch out the elements of this approach.

**Take a Comprehensive Approach.** The United States would do better in competing with China to shape the digital future if it had a coherent strategy. Competition with an authoritarian state comes as

companies are building a global digital ecosystem. This creates an opportunity to also build digital trust and development. An approach to governance based on rule of law is more likely to win support from many countries, including in Southeast Asia, than the Chinese alternative.

This is particularly true for the growing **international demand for tech governance**. A new approach to governance spearheaded by the United States can help meet the challenges from China and accommodate shifts in economic power among nations. Despite the opportunity, the United States has not done enough to lay the foundation for a rules-based approach to digital governance. There has been progress in some areas, like 5G infrastructure supply chains, but these efforts are disconnected—just a collection of regional initiatives on data and digital trade accompanied by voluntary guidelines for trust. They do not provide the scope or certainty needed for investment and policymaking and can be insufficient to forestall Chinese efforts.

Creating a governance structure is a massive undertaking, on a scale similar to the work done in the late 1940s in creating the United Nations and the IMF. A similar global undertaking is needed for the task of creating the rules to govern global connectivity and digital infrastructure. The United States, with its allies and partners, will need to define a new global architecture centered on development and trust. A compelling case for a trustworthy digital infrastructure cannot be based on the **Declaration for the Future of the Internet**, issued by the United States in 2022 and supported by only 67 partners. No Southeast Asian country was among the signatories. Appeals to return to the U.S.-centric internet of the past will be not persuasive, since they downplay sovereignty and are too Western-oriented. ASEAN officials are concerned or skeptical, and (according to some observers in the region) having seen the power that U.S. tech companies have demonstrated against Russia in the Ukraine conflict, wonder if this power might one day be turned against them.

A better model comes from the 2021 **Prague Proposal**, a set of recommendations to guide decisionmaking as countries construct 5G wireless networks. The proposal provides criteria to identify trustworthy suppliers based on public and objective evidence of a country's commitment to the rule of law, respect for individual rights, and democratic governance, as well as a company's record of respect for intellectual property protection, cybersecurity risk management, and independence from government control. They could be extended to cloud computing and networks in general. The proposal does not single out any one country but provides guidance for decisionmakers to assess the trustworthiness of an infrastructure provider based on objective criteria. Countries are more likely to accept a neutral and objective tool for risk assessment, especially if it has already been endorsed by countries like Germany and is advocated for by regionally influential countries like Japan.

This is a massive undertaking, but China has not shied away from it. China's rulers intend to build a dominant global position in technology that serves China's interests, undercuts the United States, and weakens support for rules-based democracy. Countering this requires a whole-of-government effort led by the National Security Council and the National Economic Council to develop the agenda for diplomacy and investment. The United States, working with allies, has an opportunity to structure global digital infrastructure in ways that promote rule of law, development, and sovereignty, but a new global approach will need to be backed by strategy and resources.

**Emphasize the Importance of Trustworthy Suppliers in Cloud and Digital Networks.** Southeast Asian countries have been leaders in developing regional and national measures to improve cybersecurity. They will be receptive to arguments on the need for trust to improve security and protect sovereignty. The links between trust and security can be made using the Prague Proposals for 5G, combined with efforts to build cybersecurity capacity in the region and ASEAN work on confidence building and cybersecurity. The Prague Proposals do not identify any country but suggest metrics for assessing the trustworthiness of a supplier, like the strength and independence of its courts. Events like Singapore’s Cyber Week provide an opportunity for U.S. officials and companies to put trustworthy cloud computing on the agenda for discussion with regional counterparts.

**Work with Allies Like Japan and Australia to Make the Case for Trustworthy Cloud Partnerships.** Trustworthy cloud technologies can attract businesses and investors. Southeast Asia’s start-up culture can take advantage of the increased access cloud to be more competitive. Trustworthy cloud is necessary for emerging technologies like AI, the IoT, and data analytics. Partnerships and initiatives between countries in the region, and the United States, Japan, Australia, will cross-border collaboration, standardization, and information sharing.

**Strengthen Privacy and Data Protections.** One goal for U.S. digital diplomacy should be to collaborate with allies and partners to create a global governance framework that establishes rules and standards for trustworthy networks, including data protection, law enforcement cooperation, and digital commerce. Passing domestic privacy and data protection legislation is essential to strengthening U.S. influence internationally.

Additionally, since GDPR has become the de facto global standard for data protection, with some traction in Southeast Asia, the United States needs a package of measures that would demonstrate a stronger official position on privacy. This task falls largely on Department of State and Department of Commerce to engage with Southeast Asian partners, expand existing agreements on data protection, and add new privacy protections drawn from the recent transatlantic **EU-U.S. Data Privacy Framework**. In Southeast Asia, the United States can and should build off the progress in the transatlantic privacy discussion and consider offering Southeast Asian countries protections similar to those used for transatlantic data flows. It is worth considering how measures developed as a replacement for Data Shield could be extended to regional partners. Some areas of agreement—like the Organization for Economic Cooperation and Development’s **Declaration on Government Access to Personal Data Held by Private Sector Entities**, to which the United States is a signatory—already have global application.

Southeast Asian officials sometimes raise the inability of the United States to pass national privacy legislation. Although the United States is party to regional data protection initiatives, its position would be strengthened if it could pass privacy legislation. A full discussion of the international effect of the lack of federal privacy legislation is not the topic of this paper, but the United States’ international position in this region and others would be stronger politically and commercially if it is seen as meeting international standards for privacy.

*[T]he United States needs a package of measures that would demonstrate a stronger official position on privacy. This task falls largely on Department of State and Department of Commerce to engage with Southeast Asian partners, expand existing agreements on data protection, and add new privacy protections drawn from the recent transatlantic Data Privacy Framework.*

**Streamline Foreign Assistance and Make Digital Infrastructure a Higher Investment Priority.**

The development community recognizes the importance of digitization and is shifting resources to support this. This could be accelerated by streamlining, requiring, and reprioritizing investments. In talking to officials in Southeast Asia and other regions, one complaint is that Chinese assistance appears to come with fewer strings attached. The need to streamline requirements and processes for obtaining U.S. foreign assistance processes is a larger problem that requires the involvement of Congress, the concerned agencies, and the administration. The goal is a restructuring of eligibility and oversight requirements and a paring away of conditions not directly related to digitization.

In discussions with U.S. officials, some object to reducing such requirements, saying that the goal is to ensure that the taxpayers get full value for their dollar. The metrics for “full value” have changed. The most important goals are to build support for democratic institutions, increase market share, and outcompete China in building digital infrastructure. These are more significant than avoiding waste, fraud, and abuse. Foreign assistance was a valuable tool for national security during the Cold War, but once that conflict ended, the United States reprioritized aid programs to other goals. Now, the United States needs to return to its earlier security focus in foreign assistance.

The Partnership for Global Infrastructure and Investment (PGII) may be a vehicle for moving forward. Implemented in partnership with other leading allies, PGII promises to invest \$600 billion (contributed by G7 countries) by 2027. One planned investment is for a submarine fiber-optic cable connecting the region to Europe. It is clearly intended as a counterpoint to the BRI.

The need for investment in developing countries is huge, but giving digital infrastructure a higher priority is more likely to pay off for economic growth, as this is the direction the global economy will take. This is not a request to subsidize the hyperscalers but to provide them with the political support needed to compete fairly and to provide low-income countries with the assistance in training, cybersecurity, and infrastructure needed for their development.

In Southeast Asia, there are several prominent development finance institutions that promote economic growth development. These include the Asian Development Bank, which finances infrastructure development, and the World Bank. The United States should use its influence in these organizations to promote expanded investment in trustworthy cloud infrastructure by developing conditions for trust (based on the Prague Proposals) for allocations decisions. This can be done with allied organizations, such as the Japan International Cooperation Agency or the Australian Agency for International Development.

**Expand Workforce Training.** Governments see their cloud acquisition policies as part of a development effort, including the development of a tech workforce. Training workers for the digital economy is an attractive incentive. Alibaba, for example, **has announced** that it will train one million digital workers and support 100,000 tech start-ups in the region—in Indonesia, the Philippines, Malaysia, and other countries—as part of a \$1 billion effort to grow demand for its cloud offerings. It is unclear if Alibaba is subsidized directly by the Chinese state to offer training at this scale or if it is simply a canny business investment to lock in future customers to a China-centric digital ecosystem. What is known is that a technology workforce educated on Chinese technology is more likely to buy from and work with China in the future.

Expanding workforce training should be a collaborative effort between the United States and cloud companies, with public statement committing to the number of people to be trained. In partnership, U.S. government assistance programs and company efforts can match China. AWS announced it has trained over **700,000 individuals across** ASEAN since 2017. In Indonesia, funding from the U.S. Agency for International Development helped establish a telecom training center that has trained over **10,000 telecom professionals**. The center has helped improve the skills of telecom workers and created jobs in the telecom sector.

The United States may need to consider supporting official development assistance by providing incentives and encouragement for U.S. companies to expand workforce development efforts. This requires both increased funding and a reprioritization of assistance funding goals for competition with China. There may be objections to providing tech giants with incentives for training foreign workers, but Chinese firms face no such complaints.

One option would be for the United States to establish a nonprofit foundation, modeled on the National Endowment for Democracy, to provide technology training and accelerate digitization in the developing world, building on the G7 initiatives. Even though U.S. cloud technology is attractive and can offer a broader range of services, the long-term effect of China's assistance efforts will be to ensure years of China-centric digital connectivity if the United States and its allies do not match them.

The United States has a clear advantage in one area of great interest to countries in the region: using training and assistance to build cybersecurity expertise. Offering cybersecurity training has benefits that go beyond cloud competition and can be done in partnership with allies like Australia. Countries in Southeast Asia desire cybersecurity training assistance, and providing that assistance will help make the case for trustworthy cloud services.

*The United States may need to consider supporting official development assistance by providing incentives and encouragement for U.S. companies to expand workforce development efforts. This requires both increased funding and a reprioritization of assistance funding goals for competition with China.*

***Link Trustworthy Cloud to Sustainability.*** Cloud can contribute to sustainability goals. There is reasonable concern over data centers' consumption of electricity, but this can be balanced by the contributions cloud technologies make toward creating energy-efficient infrastructure; optimizing resource utilization; and providing the backbone for initiatives like smart grids, smart cities, and precision agriculture, all of which can reduce environmental impact. Pointing to the environmental record of suppliers and their national governments can help make this case.

***Highlight the Importance of Cloud for Security Relationships.*** For those countries where the United States has a security relationship, it can help to point out in discussions with regional counterparts the potential dangers to themselves and to U.S. operations of a reliance on Chinese cloud and telecom providers. This risks being heavy-handed, but security relationships with leading Southeast Asian nations are a tool of influence the United States has that China does not. U.S. allies Japan and Australia also have close connections to Southeast Asian countries, and this can build trust and cooperation. This builds on precedents set by the contest with the Soviet Union and can be a regular point raised during visits of senior State, Defense, and Homeland Security officials.

***Reconsider Antitrust Initiatives.*** The United States must weigh the value and costs of antitrust efforts against its tech giants, taken in a purely domestic context against the damage in a global competition with China. The Chinese government, having established control over its tech companies, now uses them as a tool of international influence. The United States should do the same or it will put itself at a disadvantage. As with foreign assistance, the United States still has not reprioritized its policy for a global competition with a powerful authoritarian state. For this conflict, well-regulated U.S. industry leaders better serve the United States in the competition with China.

***Improve Regional Trade Policy.*** For Southeast Asia, actions that promote trade and give them greater access to the U.S. market are more persuasive than military security arguments. Countries in the region gauge U.S. influence and staying power with economic and trade metrics. Not joining the Indo-Pacific Economic Framework for Prosperity (IPEF), the Regional Comprehensive Economic Partnership, or the Comprehensive and Progressive Agreement for Trans-Pacific Partnership is damaging to the competition with China, which has no such reluctance.

It is impossible to reach agreement on membership in Congress and with the administration, particularly in an election year, and some erosion of the U.S. security position in the region should be expected. Cooperative efforts in development and security can compensate for this, and the United States must find compensatory steps short of membership. U.S. support for regional trade agreements sends an important message to countries in the region, who sometimes have qualms about U.S. commitment and consistency. The IPEF may provide partial improvement by demonstrating a U.S. commitment to the most important concerns for countries in the region.

### ***Success Requires A Comprehensive Approach to Cloud Competition***

This is a long list of actions. They form a wide-ranging package for building a trustworthy digital order in Southeast Asia and other regions. Progress on even a few of these recommendations would help in the competition with China and would help ensure that the foundations of digital connectivity are trustworthy.

For Southeast Asia, actions that promote development and growth are more persuasive than military or security arguments, and this is true for much of the Global South. This is not a commercial competition between rival companies taking place within the framework of the rule of law; it is a competition between a powerful authoritarian state and its national champions. The future security of the United States depends on building a trustworthy global digital infrastructure where U.S. CSPs play a central role. This requires a whole-of-government approach guided by a strategy that blends technology, economic, and security initiatives in ways that provide for success in the new international environment.

The role cloud computing plays in international relations is not always apparent. Cloud computing is not a fashionable tech concern, and its foundational importance for influence in the emerging digital world is not always recognized. But the nation that builds the global digital infrastructure—in which cloud computing is the backbone—will gain tremendous advantage in shaping the course of the digital future. ■

*James A. Lewis is senior vice president, holds the Pritzker Chair, and director of the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C.*

*The author would like to thank the anonymous reviewers for their assistance.*

*This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.*

**This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax- exempt institution focusing on international public policy issues. Its research is nonpartisan, nonrandom, and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).**

**© 2023 by the Center for Strategic and International Studies. All rights reserved.**