APRIL 2023

An Overview of Global Cloud Competition

By James Andrew Lewis

In the nineteenth century, industrialization reshaped national power as it drove economic growth and technological change. Digitalization will do the same in this century. Digitalization is the use of computing technologies to change how we produce and communicate. The technologies include terrestrial and undersea fiber-optic cables, satellites, mobile telecom (including 5G and 6G), along with the internet protocols and standards that let them interoperate. These provide the infrastructure (both physical and software) for digitalization.

Digitalization has become central to the strategic contest with China, given its importance for economic growth. It creates what Zbigniew Brzezinski called (in 1997) "novel dimensions of power." U.S. foreign policy must take these new dimensions into account. Cloud computing is the foundation of digitalization. Cloud computing is reshaping economies as business take advantage of the benefits it provides for cost, security, and performance. As such, cloud computing has become a focus for policymakers and another area of geopolitical competition as tech governance, sovereignty, and economic competitiveness become major political issues.

The cloud is simply a computing infrastructure that can be accessed remotely, along with the data stored on it, the software that runs on its infrastructure, and the services it provides. Cloud computing is about services and data—digital information collected and organized to guide analysis—where it is stored, where it is processed, and what laws govern its use.

Cloud services play a crucial role as the backbone technology. Other emerging technologies, such as robotics, autonomous vehicles, biotechnology research, 5G, and artificial intelligence, depend on the cloud, making it truly strategic. The development of cloud services and infrastructure is a strategic issue in that the outcome of cloud competition will shape the economic and security environment for the United States and other democracies.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

> *Digitalization has become central to the strategic contest with China, given its importance for economic growth. It creates what Zbigniew Brzezinski called (in 1997) "novel dimensions of power." . . . Other emerging technologies such as robotics, autonomous vehicles, biotechnology research, 5G, and artificial intelligence, depend on the cloud, making it truly strategic.*

Decisions by governments, companies, and consumers about which cloud providers to use will shape commerce, global influence, and international security. There is a growing competition between China and the democracies over who will provide the infrastructure, technologies, and services that will drive the economies of the future. Societies depend on the cloud (even if they are sometimes unaware of this) for key services, and it has become a battleground for international influence in the contest between democracies and authoritarianism.

Countries in Latin America, Africa, and the Indo-Pacific—but also in southern Europe—are moving into a Chinese sphere of economic and technological influence. Although China's share of the cloud market beyond its borders is currently small, the intent is to expand it as part of a larger effort to build and control the foundations of global connectivity and, with it, gain a dominating position in the global economy.

An example from history comes from nineteenth-century Britain, with its leading position n global shipping, finance, and telecommunications. These "networks," along with a strong domestic industry and a powerful fleet, underpinned Britain's global leadership. The United States is not the British Empire, but in 1945 with its allies, it was able to create a global order based on democracy, markets, and the rule of law. China now intends to replace this order, and leadership in digitalization will help determine the outcome of this contest.

The competition over the cloud is in many ways a continuation of the earlier contest over trustworthy 5G telecom infrastructure. The similarities to the 5G battle are telling. It took several years for the policymaking community to revise the Western approach to 5G to make it more competitive and to emphasize trust. The 5G competition is a useful precedent and the United States is on the same path when it comes to the cloud.

One obvious area of strategic significance involves espionage. Cloud service providers hold data, and there are fears (reasonable in the case of China) that they can gain access to stored data without the owner's consent. Even if the data is encrypted, the metadata on patterns of use may provide intelligence benefit. China has a record of doing this kind of collection of both data and metadata, and its **well-known national intelligence law** makes it incumbent on Chinese service providers to cooperate with any government request. Ever since the **2013 Snowden revelations**, similar charges have been leveled against the United States, but there are significant differences. U.S. service providers want to protect their global market by establishing their independence from government agencies and, unlike Chinese companies, have the legal standing to challenge any government request in independent courts.

The United States also does not engage in the commercial espionage that is widely and reasonably **attributed** to China. Espionage is a central element of China's economic and foreign policies. China

uses espionage not only to acquire intellectual property but also (according to several Western intelligence services) to acquire confidential business information to help its companies in trade deals and contract negotiations. In contrast, as the Snowden revelations showed, U.S. intentions focus on security. U.S. surveillance was carried out for counterterrorism purposes, usually in cooperation with and at the request of partner and allied governments. As recent agreements with the European Union and the Organization for Economic Cooperation and Development (OECD) show, it better serves the national interest of the United States to make concessions that limit any collection. The risk of espionage points to the advantage of having trustworthy cloud service providers who operate under the rule of law.

The policy framework for cloud competition revolves around two concepts: development and sovereignty. These must be the foundation for U.S. policy. Decisions on data localization and trustworthiness raise important questions for national policy. Exclusionary or protectionist policies will harm economic growth and security, and this harm will only increase as the digital transformation progresses. Companies that do not make use of the best cloud services will be at a competitive disadvantage. Companies that use cloud services where there is risk of compromise create cybersecurity and innovation risks for themselves and their nation. An untrustworthy cloud service provider can create technological or economic dependence and bring with it the risks of interception or disruption of data.

Although the United States' primary concern is security, other countries are driven by concerns of equal, if not greater, importance. For countries in Africa, South America, and Asia, the most important issue is economic development. They do not dismiss the risk of using untrustworthy equipment and services but believe that the risk is outweighed by the prospect of faster development, even if provided by using untrustworthy infrastructure. These countries are motivated by the imperative for development, accompanied by lower prices and the provision of assistance. Appeals to security alone will be inadequate to counter this.

Chinese providers offer cloud services that are a product of China's state-centric industrial policies, and these policies serve both China's commercial and security goals. Western providers say China's cloud services are currently of a lesser quality, but this is not a compelling argument. In fact, they are more than adequate for many business and government tasks. Given China's financial support to its companies, market forces alone will not protect its security and the security of its allies. If it is to build a trustworthy global infrastructure, the United States needs policies that address both development and sovereignty and create the basis for fair competition over the provision of cloud infrastructure and services. These are not conventional trade issues, so conventional trade and security strategies will be inadequate. These are political and economic issues that require creating a new diplomatic agenda to address technology and trust if the United States and its allies are to succeed in ensuring the emerging global network is reliable and secure.

The Importance of Development

Although the United States can make a compelling case on the security risks of using untrustworthy technology, it is not compelling enough to dissuade many countries and companies from relying on Chinese technology. To do this effectively, U.S. warnings on security should be accompanied by complementary strategies for development, with government assistance focused on achieving strategic

goals intended to improve security. Discussions with officials from developing world governments make clear that economic development, rather than national security, is their chief priority. U.S. policy and the policies of its allies should make the case that development is more durable using markets based on the rule of law and then back this up with funding. Without funding, words are insufficient.

This is not an unprecedented move but rather a return to the tools used in an earlier conflict. Starting with the **Marshall Plan**, this security rationale was one of the central motives for foreign assistance, but since the end of the contest with the Soviet Union thirty years ago, the United States let this tool of strategic influence weaken. Development aid needs to be focused on the strategic goal of protecting an international system based on the rule of law as part of a long-term contest with a hostile authoritarian power. There have been good steps in this direction, but it is too early to tell if they have traction or are of sufficient scope.

China's counterargument to a model of markets based on the rule of law is its success over the last 40 years in going from poverty to wealth using an authoritarian alternative to this Western model. China leaves out important elements of the story—its commercial espionage and the massive investment by Western companies—that will make it difficult for others to emulate. But China's success, combined with its subsidies and assistance, help make a case for Chinese companies. Although China's **Belt and Road Initiative** (BRI) has been scaled back and is now often viewed with distrust in some developing countries, China's blend of assistance and investment remains potent as a tool for expanding influence in the face of little Western competition.

The United States and its allies have, in many ways, ceded the field to China. Overall, **development assistance** for communications declined 25 percent in 2006–2019. It now makes up just 2 percent of total infrastructure spending. China has taken advantage of the opportunity created by this decline. China typically provides development finance in the form of loans, often at highly subsidized rates. The contracts generally stipulate that the recipient country must spend a large share of the money with a Chinese firm, which provides all materials and much of the labor—particularly skilled labor—needed to complete the project. Although the luster of the various Chinese foreign assistance programs has dulled given problems with the quality of construction and the debt problems created in poorer recipient countries, they remain attractive in the absence of Western competition.

One major obstacle for competing with China is that U.S. rules and regulations for foreign assistance have become obstacles. The United States became unaccustomed to competition after 1990, and many of the foreign policy tools it used for influence, development, and security in the Cold War were dismantled, diminished, or repurposed for other social goals. U.S. assistance rules limit the countries that can receive aid and impose conditions that some countries find to be onerous. China does not impose similar conditions and requirements, making it easier for countries to work with them. These well-intentioned rules were not designed for a contest with another power and can hamper the long-term strategic goal of building trustworthy networks in friendly nations. Frankly, these rules make security a secondary concern for foreign assistance.

Additionally, the United States has not tried to modify how funding is allocated by international financial institutions (like the World Bank or Inter-American Development Bank). Ironically, U.S. contribution to these development banks sometimes ended up funding projects from Huawei, China's global IT champion, in part because of the emphasis on buying at the lowest cost. This needs to change

and other criteria, such as trust and security, must take precedence. Changing rules to make foreign assistance funding for communications infrastructure more flexible and better aligned to today's security environment must be a priority.

China now uses tools of influence similar to those the United States used in the Cold War to gain long-term commercial and security advantages. China typically provided **development finance** in the form of loans, at either highly subsidized or market interest rates, for large infrastructure projects. Chinese programs are scalable and can support small projects that private Western companies would not be interested in. Assistance is not accompanied by political considerations but rather is focused on producing economic advantage for China. These programs are as much assistance to Chinese firms as to foreign recipients. Chinese companies also provide training and technology education to recipient countries, which is very attractive to many governments. Huawei has set up schools and training centers in more than a dozen countries. While some of China's aid programs have run into problems, this does not translate into U.S. success.

Western development agencies may argue that they are already providing education and training. Even if that is true, they are not doing it at the scale or pace needed to compete with China. The United States does not need to match China dollar for dollar, but it needs a comprehensive response to China's efforts to shape the global infrastructure that addresses the concerns of other nations (chiefly, economic development and respect for sovereignty). The "**Partnership for Global Infrastructure and Investment**" initiative is a strong start at recovering U.S. influence, provides the opportunity to work with G7 partners, and should be rapidly expanded.

China in the Cloud

China knows that there is strategic advantage for the country that builds the world's networks. It has invested billions of dollars over the last two decades to create technologies and build companies to do this. The Chinese government is willing to do things that do not make business sense in order to dominate the information infrastructure. It knows there are immediate commercial, political, and intelligence benefits to providing cloud infrastructure, and there is long-term benefit to Chinese vendors and manufacturers from the country that supplies that infrastructure.

An infrastructure built to Chinese standards makes it more likely that China's cloud customers will in the future use Chinese technology—creating what is, essentially, a world connected and operated by China. China has a central, if not dominant, position in the digitalization of Africa and growing strength in other regions, particularly Latin America and Southeast Asia. Even in Europe, despite countries turning away from Chinese telecom suppliers, many nations still rely on earlier generations of Chinese network technology.

> *Countries in Latin America, Africa, and the Indo-Pacific—but also in southern Europe—are moving into a Chinese sphere of economic and technological influence. . . . China knows that there is strategic advantage for the country that builds the world's networks.*

While China knows there is strategic advantage in networks, the United States was slow to recognize this. This slowness reflected rosy assumptions about bilateral relations that guided U.S. policy toward China until recently, accompanied by decisions to rely on private investment rather than government-funded programs. This may have been acceptable before the contest with China began, but China's ambitions create strategic risk. The contest is distorted even more since it is between private companies in the West and **government-subsidized companies in China**. China is building a dominant position in telecom infrastructure across much of the world that will be impossible to displace in the near term.

The U.S. advantage in this competition is that its technologies are better. Its companies have the **majority share of the cloud market** because of this, but several trends put leadership at risk. China's advantage is that its cloud offerings are part of an integrated development package intended to build China's international presence and influence. This integrated package includes training and education for capacity building, technical support, and **subsidies** for telecom and cloud infrastructure. In the same way that the Chinese government used Huawei to drive Western companies from the telecom market by offering subsidized prices, it plans to drive Western suppliers from the cloud market. Without changes to U.S. policy, the subsidies and support that drove Huawei to network dominance in the developing world could restore its position and ensure China's network dominance for cloud and next-generation telecom.

Huawei was built on a foundation of industrial espionage, government subsidies, and close ties to and support from the Chinese government. Until the United States intervened to warn other countries about relying on Huawei, it was on a path to becoming the globally foremost supplier of telecom. Although this effort has been blunted, and the company's brand damaged, Huawei still supplies the majority of telecom infrastructure equipment in the developing world. **Huawei expects** to restore its dominant position by creating 6G network technologies and expanding its footprint in the global cloud market.

China's presence in the global cloud market is small, but it is growing and is part of a larger comprehensive, long-term effort. If Chinese cloud providers like Huawei were based in any country other than China—with its pursuit of an authoritarian, Chinese-dominated global order—there would be no grounds for complaint. The issue is that this new competition is accompanied by both predatory trade practices, such as subsided prices (China has never felt particularly bound by its World Trade Organization [WTO] commitments), and significant political risks from espionage and coercion.

Even though U.S. companies are competitive in the cloud market, U.S. policy is not. The need to compete with Chinese telecom suppliers now has wide recognition, but there has been little attention on the need to compete in cloud services, as well. There is the U.S. preference to rely on markets and the private sector. This market orientation is usually justified, but not in a state-versus-state conflict. The Chinese state does not regard itself as bound by Western norms or the rule of law. This means

that Chinese companies are not normal competitors. The Chinese government plays an intrusive and directive role in companies' affairs to meet China's strategic goals. This allows it to use a Chinese company for espionage or coercive purposes, and in some cases, control and censor information. Subsidies and government investments increase Chinese international influence by providing developing countries with needed infrastructure at a subsidized price. China's advantage is not just subsidized prices. Subsidies allow **Chinese companies to offer training and research** to hundreds or even thousands of students in customer nations, often at a scale that dwarfs Western efforts, and China uses this assistance to gain influence and promote its view of a China-centric world. Support for digital infrastructure is what China would call a win-win.

These Chinese state investments occur in the context of growing international concern over Chinese technology practices. There are fears that the Chinese government is attempting to capture the standards process to cement demand for Chinese technology and is working to restructure the open internet to make it more state friendly. Chinese government overseas infrastructure and development projects—broadly represented by the **Digital Silk Road** and the BRI—are intended to increase China's global influence. This includes the spread of Chinese surveillance technology whose output can often be accessed by Beijing. The overall effect is to increase technological dependence on China and its political influence. In the Global South, China challenges Western firms for leadership of the telecom and cloud computing market. This challenge requires solutions that provide development aid, address sovereignty concerns, and ensure open and fair technology competition (for example, in **standards-making processes**).

Even though China increasingly holds a dominant position in telecom infrastructure across much of the world, two technologies may be able to erode this dominance. The first is open network technologies (like Open Radio Access Network) that will replace traditional telecoms infrastructure over the next 10 years. The second is cloud computing, available now and that changes architectures and infrastructures in ways that can reduce risk. The two are closely linked since open network technologies depend on cloud computing—5G and later-generation networks do not work without the cloud. Huawei recognizes that this dependence on the cloud could be a risk to its business, which is one reason why it is emphasizing cloud and next-generation telecom.

Many believe that China hopes to dominate the global communication infrastructure because it will help build a China-centric world order and undercut the appeal of the rules-based, market democracy model that the United States and others advocate. There should be no doubt that a global infrastructure built by China will provide it with political, commercial, and intelligence advantages. The challenge for the market democracies is to respond to this through action and results (and not merely speeches) that show their approach is superior.

Sovereignty and the Cloud

Competition with China is only part of the new international environment that U.S. policymakers must manage. The world is no longer bifurcated between East and West, and the interconnections among nations are deep. It is not just competition with China and its support for economic development in the Global South that will shape the global infrastructure, but also the strong desire in many countries to protect their national sovereignty. Countries want to protect their sovereignty and see this as a way to also gain more of technology's economic benefits. The resurgence of sovereignty over the last decade

(and the concomitant decline of U.S.-led globalization) has reshaped international politics and with it, national views on cloud competition.

Sovereignty is the ability of a nation to decide its own course of action and make decisions independently, consistent with respect to national laws and institutions. There has been a resurgence of national assertions of sovereignty in international relations in the last decade. This reflects a general reaction to globalization, which is seen as eroding national prerogatives and control.

> *Competition with China is only part of the new international environment that U.S. policymakers must manage. The world is no longer bifurcated between East and West, and the interconnections among nations are deep.*

The operations of the internet do not follow geographic boundaries. If the 1990s ideals underpinning globalization were that the internet would help build a borderless world based on American values, other countries now reject them (in varying degrees). Cloud services, by their nature, work best in an environment where data can flow easily across borders, but data and tech sovereignty initiatives are designed to do the opposite. The purists of greater sovereign control of digital and tech resources will become part of the larger retrenchment of U.S. global influence unless the United States finds ways to respond to and shape the new international dynamic.

The desire to protect national sovereignty has become a central shaping factor in the discussion of technology and internet governance. Nations were willing in the past to cede sovereign control in some cases—usually on specific and defined issues such as trade, finance, or human rights—through accepting a binding international agreement. The internet, with its cross-border technologies, created the greatest challenge to national sovereignty in decades. The first few years of internet use saw rapid growth in transnational connectivity, driven by deployment and use without regard to political borders. Now that the world is connected, the trend for government policy is to seek greater sovereign control of the digital environment.

Sovereign control often involves data localization—laws and regulations that restrict data transfer across borders and compel companies to store data within a country's territorial jurisdiction, provide procurement preferences for national companies, and restrict the ability of foreign companies to compete in their markets. Sovereignty is Europe's leading concern when it comes to cloud competition, but other regions share this concern to varying degrees.

Many countries are establishing national cloud service or data localization requirements to protect sovereignty and to create, they hope, economic benefit. Paradoxically, some of these sovereignty-motivated projects, especially in developing countries, are financed, constructed, and even operated by China in ways that build dependence on it.

Cloud technologies create a transnational digital environment that enables growth but raises national sovereignty issues since the largest clouds—the "hyperscalers"—are built on global networks that span national borders. The U.S. hyperscaler cloud service providers offer cloud services where efficiency

and cost determine location since it can put data and infrastructure outside of sovereign control. These transnational clouds are more efficient and more secure, but countries seek to ensure data sovereignty using regulations and limitations for cross-border data flows. This creates an immediate tension between the desire to ensure sovereign control over digital resources and the economic benefits of openness and connectivity at scale. This tension will increase as governments and companies increase their reliance on cloud services.

Protecting sovereignty has broad appeal, particularly in Europe. More than **60 countries** (including the 27 members of the European Union) have passed laws restricting the flow of data across borders. Personal data is the most common form of data that countries restrict from leaving their borders, followed by financial and government data (which includes public records, defense data, and tax and debt data). Access to content is one reason why analogies to the late-nineteenth-century competition over undersea cables are imperfect. Cloud services are different from other infrastructures like highways or dams because cloud infrastructure stores and manages data—information on people, businesses, and governments.

The European Union is the most prominent example of the pursuit of data sovereignty, with a few **of its members** even adopting questionable technology transfer and procurement mandates that mirror those used by China. At **least one EU country** has adopted Chinese-style policies for forcing technology transfer and requiring majority owners by a national company. The draft **Cybersecurity Certification Scheme for Cloud Services** (EUCS) includes sovereignty requirements (despite objections from some member states). Chinese and U.S. companies are willing to accommodate data localization if the size of the country's market justifies it, but this comes with an economic cost for both the host nation and the service provider, since this kind of protectionism has proven to be more cumbersome, expensive, and slow in providing new features.

Distrust of U.S. technology can serve as a rationale for localization and protectionism but in fact, the physical location of data does not determine its security. **Some officials** seem to believe that location mandates will create incentives for innovation and better security. The United States needs to address this new protectionism by countering allegations of mass surveillance, by promoting regulatory parity, ensuring its companies' independence, and engaging in negotiations that build on the successful work in the **talks to replace the EU-U.S. Privacy Shield framework** and in the OECD on governing extraterritorial requests by law enforcement agencies.

The terms of protectionism have shifted from tariffs to a new set of regulatory barriers built around privacy and cybersecurity. Even though the justification for protectionism has changed, the effect is the same: obstacles to open and fair trade. The Snowden incident is used to justify blocking data transfers to the United States, but it has become more of a **rationalizing fable** than an accurate depiction of risk. The disadvantage for the United States is that since it has removed most of the barriers for twentieth-century products (where Europe is strong), it has less leverage over twenty-first-century products (intangible goods and services).

Overextension of sovereignty also raises security concerns. Ukraine used third-party hosting arrangements to move some data and services outside of its geographic boundaries at the onset of the conflict with Russia and was forced to rapidly amend localizing laws. If nothing else, this extraterritorial

hosting complicated and constrained Russian planning. Data localization can come at the expense of resilience. Attacking these remote services located in third countries poses the risk of repercussions an attacker may prefer to avoid.

Protectionism cannot be the goal for cloud and data governance. This means finding through negotiation some system of jointly agreed upon (rather than unilaterally imposed) regulations that allow institutions to move data freely outside the originating jurisdiction when they can ensure the security and privacy of their customer data. Both sides need each other in the growing contest with authoritarian regimes. Each depends on the other as a market and as a security partner. This interdependency will only grow as the risks of trade with a predatory China increase for both.

European politics complicate cloud competition. In Europe, there is a deep concern over personal privacy, now accompanied by greater attention to cybersecurity. These are important topics, but they are sometimes used as a disguise for cloud protectionism. This is accompanied by a kind of industrial policy that restricts U.S. cloud service providers in an effort to restore the European tech sector (**and for at least one EU member, to hold back the United States**). However, attempts to create a European cloud alternative (Gaia-X) have fallen victim to European infighting. Regulations and review requirements hamper U.S. service providers but also make European companies less efficient and slow European digitalization. The ultimate solution may lie in the development of new trade policies for the digital economy by moving beyond the classic trade agenda and for the United States to engage Europe in specific dialogue with concrete proposals for negotiation.

The balance between development and sovereignty as shaping factors for cloud competition will vary from market to market. In Europe, concern for protecting sovereignty (and restring economic growth) will play a greater role in policy choices, in part because this is a political focus for important members of the European Union. Economic development is the priority in Africa, Latin America, and Southeast Asia, though these countries also wish to protect their sovereignty. Cloud technologies are most efficient when they allow cross-border data flows and create a reasonable desire to balance sovereign control over digital resources against the economic benefits of openness and connectivity at scale. Finding this balance is not easy, and the costs of inefficient cloud infrastructures are not always apparent.

RESOLVING THE SOVEREIGNTY DISPUTE WITH EUROPE

Progress in resolving disputes over technological sovereignty would be one of the most important steps the United States could take for its national security. It is in the United States' interest for Europe to be wealthy and strong, as having a strong and wealthy democratic partner that observes international norms and is committed to the rule of law is essential for the United States. Europe's leadership in digital governance is one reason why it is an essential partner.

The politics of both transatlantic and intra-EU relations complicate efforts to address the problem quickly. Although some of the European Union's founders hoped it would create a confederation of European states that one or another of the larger European powers could direct, the European Union is also hampered by sovereignty concerns. These concerns prevent a clear delegation of power to Brussels in key areas, particularly in national security.

This creates a complex diplomatic landscape where the United States will need to engage with the Europeans on multiple levels. Finding persuasive arguments that win support for a mutually beneficial response to the sovereignty issue requires a multifaceted approach, a negotiating process, and a menu of possible concessions. Although a good case can be made that the pursuit of digital sovereignty risks harming European economic prospects, straightforward economic arguments will not address the political issues behind the pursuit of greater sovereignty. It is worth laying out this economic case for European consideration, but by itself, it will be inadequate. Appeals to reject protectionism and support open trade may face additional obstacles after the passage of the Inflation Reduction Act (IRA).

A security argument, though strengthened by Russia's invasion of Ukraine, will also not be adequate. There is some European ambivalence over China and a desire for continued trade with China among some EU members. This could change if China's behavior becomes even more troubling, but Brussels does not have the responsibility to protect national security and has tended to prioritize economic issues and competition with the United States. A better approach would be to challenge EU actions as contrary to their WTO obligations. Although new EU regulations for cloud and digitalization are on shaky legal ground and should be challenged in court, the real issue is the intent that drives them, and this is what the United States must address.

To fully address concerns over espionage, the United States needs to rebuild trust that it is not engaged in mass surveillance. This may involve greater transparency, political commitment, and perhaps new legislative guard rails to address foreign concerns. There has been real progress in this direction, starting with a December 2022 agreement in the OECD on the **Declaration on Government Access to Personal Data Held by Private Sector Entities**, which identifies principles to guide protections that governments will create for individuals' data. The OECD agreement followed the United States' issuance of Executive Order 14086 Enhancing Safeguards for United States Signals Intelligence Activities on October 7, 2022. Implementation procedures for Executive Order 14086 were issued in **guidance** from the Director of National Intelligence and by the Justice Department's creation of a Data Protection Review Court. The United States also took steps to implement the EU-U.S. agreement on a new **Trans-Atlantic Data Privacy Framework**, created in response to the European Court of Justice's decision to strike down an earlier U.S.-EU agreement on data sharing. These actions significantly reorient the environment for transatlantic cloud policy and regulation in ways that make transatlantic sovereignty concerns easier to manage and could set precedents for other countries.

Several other initiatives also point to progress—Japan's **Data Free Flow with Trust** proposal, the OECD's declaration discussed previously, the new EU-U.S. Data Privacy Framework, and the transatlantic **U.S.-EU Trade and Technology Council** (TTC)—show a recognition of the need for a common approach to data flows and for an agenda no longer defined by classic trade issues like tariffs. The May 2022 TTC **joint statement** on deliverables included language on the importance of addressing security risks from high-risk vendors and fostering security, diversity, interoperability, and resilience across the digital technology and services supply chain. The **December 2022 TTC statement** pledged to expand coordination on financing digital infrastructure projects in third countries, beginning with a memorandum of understanding between the United States International Development Finance Corporation and the European Investment Bank to enable increased collaboration on financing secure connectivity in third countries as part of the larger U.S. and EU

global development initiatives. These agreements create the basis for agreement on digital trade and management of the cloud to maximize opportunity.

> *To fully address concerns over espionage, the United States needs to rebuild trust that it is not engaged in mass surveillance. This may involve greater transparency, political commitment, and perhaps new legislative guard rails to address foreign concerns.*

Modernizing U.S. Policy for Global Competition

Data has become a leading source of economic advantage, and data governance is a focus for policymaking. Cloud services are at the center of this for both economic and national security. Owning and operating cloud infrastructure creates a pressure point if the country controlling the operators uses this for coercive political purposes—slowing or denying access to important data during a crisis, for example. Control by a hostile foreign power such as China can put a customer nation at a disadvantage.

Given the central importance of the cloud, badly designed policies will harm economic growth and security globally, not just in the United States or Europe, and this harm will only grow as digitalization progresses and as the nature of foreign policy is reshaped by technology. Companies that do not make use of the best cloud services will be at a competitive disadvantage. Companies that use cloud services where there is a risk of leakage or compromise create cybersecurity risks for themselves and their nations. Simply arguing for free trade in cloud services will be unpersuasive for a global audience, but adding layers of protectionism promises only economic harm. The answer must emerge from negotiations on data governance rules that protect both competitiveness and privacy, and this will require concessions from all parties.

The United States made an immense effort, with some success, to dissuade countries from using Chinese suppliers for their 5G infrastructure. This success will be of limited value if Huawei and other Chinese companies become the main suppliers of cloud infrastructure and services. Service for 5G depends on the cloud, and the cloud encompasses much more than infrastructure. Not using Huawei for 5G but relying on them for cloud services merely changes the source of risk. If current trends continue, Chinese influence will grow, and U.S. influence will diminish. What can the United States do in response if it is unwilling to accept this outcome? There are five steps the United States should take:

1. Increase foreign assistance funding levels to support digitalization in developing countries and amend the rules for providing assistance for telecom and cloud services to make assistance more flexible and less subject to restrictions. National security should again be the primary objective for providing assistance.

2. Rebuild trust by addressing concerns over data protection (and this might require passing national privacy legislation) and further develop common understandings and principles with allies and partners for trustworthiness and competitiveness, perhaps by expanding and applying the **Prague Proposals** to include cloud services.

3. Implement a comprehensive strategy with foreign partners for diplomatic engagement and financial assistance in developing nations based on promoting development and respect for sovereignty. Building a trustworthy cloud and telecom infrastructure is best approached multilaterally, both to share costs and to increase international support.

4. Further develop a new negotiating agenda for technology and trade with key applies, and Europe in particular, that is designed for twenty-first-century economies, which rely on intangible goods and services delivered by the internet, and that directly addresses the issues of digital protectionism and data protection.

5. Make an agreement on an open and transparent cloud competition to build trusted cloud and telecom infrastructure a central a part of new economic initiatives like the Indo-Pacific Economic Forum and the Americas Partnership for Economic Prosperity.

This package of measures addresses the chief concerns of cloud competition. The goal for U.S. policy should not be to block China or dominate global infrastructure but to use the emerging structure of fiber-optic cables, satellites, next-generation telecom, and cloud to promote development, security, and trustworthiness and to ensure that the policies governing it are transparent, fair, and based on the rule of law. This makes setting the rules for cloud competition a central part of a new global negotiating agenda for the United States.

> *The United States made an immense effort, with some success, to dissuade countries from using Chinese suppliers for their 5G infrastructure. This success will be of limited value if Huawei and other Chinese companies become the main suppliers of cloud infrastructure and services.*

Creating policies that promote U.S. interests in the global cloud competition is part of a larger adjustment for U.S. policy to fit a competitive international environment. Military power is no longer sufficient to advance U.S. interests. In a long 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. In the 1950s and 1960s, as the United States confronted a hostile, authoritarian competitor, it assembled not just the military power but also the diplomatic, economic, and informational tools of influence needed for its security. It needs to do this again to prevail in a new and more difficult and complex contest. The cloud has not received the degree of attention from the policy community it deserves. But answering the fundamental issues it poses—trust, sovereignty, and development—can create a new approach to foreign policy. ■

James A. Lewis *is a senior vice president, holds the Pritzker Chair, and directs the Strategic Technologies Program at the Center for Strategic and International Studies in Washington, D.C.*

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