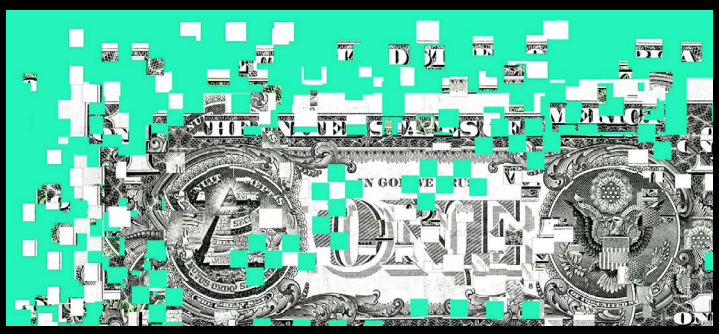
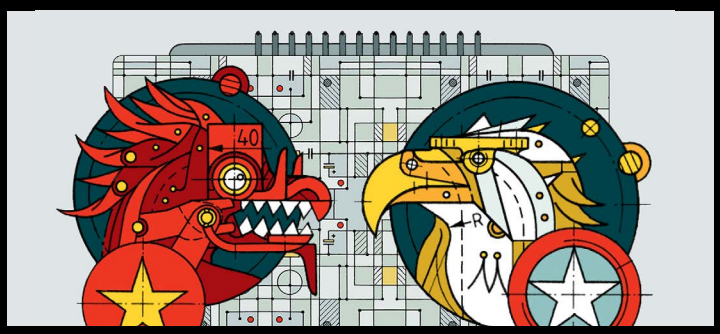
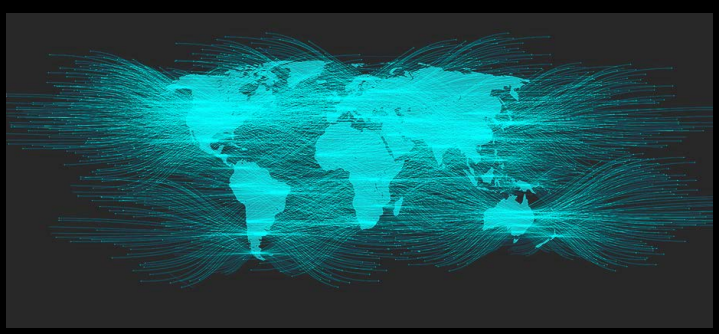
FP insider

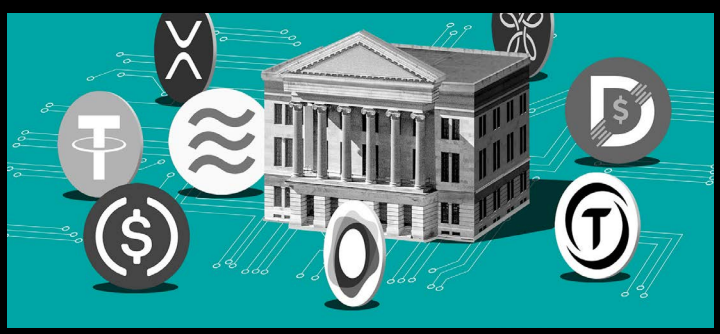
Actionable Intelligence for a Changing World

The latest briefings from FP Analytics on Russia sanctions, crypto regulations, semiconductor supply chains, and other global developments shaping business. Access FP Insider's full portfolio of analysis by becoming a member.









FP insider

Combined with full access to *Foreign Policy's* leading journalism, FP Insider provides exclusive access to research from FP Analytics that provides insightful, data-driven, and actionable intelligence on transformational trends impacting geopolitics and business. FP Analytics research, produced exclusively for Insiders, distills major topics such as 5G, data governance, and resource competition; identifies geopolitical and competitive forces shaping markets; and highlights risks and opportunities for businesses and organizations operating around the world.

PUBLISHED ON MARCH 17, 2022

How Will New Export Controls Impact the Global Semiconductor Shortage?

The U.S. mirrors tactics used against China on Russia as war in Ukraine escalates.

A worker in a dust-proof suit controls an LED epitaxy chip production line at a semiconductor workshop in Nanchang, in China's Jiangxi Province on Jan. 26.
COSTFOTO/FUTURE PUBLISHING VIA GETTY IMAGES

By **Gahyun Helen You**,
Policy Analyst with FP Analytics

The scale and combination of coercive economic measures imposed on Russia by a growing coalition of states in response to Putin's invasion of Ukraine are unprecedented. On February 24, 2022, forty-nine Russian and two Belarusian entities were added to the U.S. Bureau of Industry and Security (BIS) Entity List, effectively cutting them off from accessing key U.S. technology, including semiconductors.

Semiconductors (or chips) are the lifeblood of modern technology, enabling devices from smartphones, to automobiles, to hypersonic weapons. In addition to the direct measures against Russia and Belarus, the United States, its allies, and major producers in the semiconductor supply chain have imposed similar export controls on other countries and companies that are supporting Russia's military campaign in Ukraine. The new restrictions could choke off the Russian economy's access to Western technology and devastate sectors critical to its economy, including energy, defense, aerospace, maritime, and telecommunications—all of which depend on the essential chips.

These latest developments are set against the backdrop of record inflation and global supply chain bottlenecks, with firms around the world grappling to recover from the pandemic. In the automotive industry alone, chip shortages cost companies $210 billion in revenue in 2021, and losses are set to get worse. The U.S. Department of Commerce reports that due to limited chip supply, companies are holding less than five days' worth of inventory compared to forty days in 2019. Any additional shocks to the supply chain could further undercut companies' output and revenue.

In his first State of the Union address, President Biden urged Congress to pass legislation to support $52 billion worth of federal investments and tax credits for domestic semiconductor research, development, and manufacturing to meet surging demand. The call is part

of the administration's effort to maintain U.S. leadership in the semiconductor manufacturing, boost domestic manufacturing, and strengthen competitiveness. Notable are Intel's plans to build a $20 billion chip factory in Ohio which could increase to $100 billion over the next ten years with federal support. However, even with government incentives, given that it takes on average of three to five years to build one manufacturing facility, it will likely be years before U.S. firms can ramp-up domestic manufacturing.

How we got here, the implications of export controls on Russia, and the potential impacts on the semiconductor supply chain and the global economy are discussed below.

The U.S. applies its China export control strategy to Russia

U.S. export controls typically regulate the flow of technology to foreign adversaries that are deemed by the president and Congress to pose national security risks. To deter Putin and undermine Russia's military campaign, the Biden administration is strategically leveraging a relatively new tool in the United States' economic toolkit—the foreign direct product (FDP) rule.

The FDP rule requires that foreign firms obtain a license for any dual-use products (or commercial technology that can have a military application) that rely on U.S. technology or software. The rule was notably utilized under the former Trump administration to target Chinese tech firms, specifically Huawei, by banning any chip sales to the tech giant if U.S. semiconductor manufacturing equipment or software was used during the production process. Given the United States' dominance in the chip supply chain, this action virtually cut off Huawei's access to semiconductors.

As compared with the rules imposed on Huawei, the export controls and FDP rule imposed on Russia and Belarus are far more extensive as they cover a wider range of products and restrict the flow of any foreign items made with U.S. technology or software, except for food and medicine. In effect, the rules prohibit a suite of items that potentially have a military end use and rely on U.S. technology, software, or equipment, such as semiconductors, from being sent to Russia or Belarus.

When the FDP rule was applied to China in 2020, industry groups criticized unilateral action by the United States as the move applied extraterritorial reach of U.S. law on foreign firms. Skeptics raised concerns that it would deter firms from doing business with U.S. companies as foreign firms were required to abide by U.S. restrictions if they also relied on any U.S. technology or software. However, unlike with China, the rules imposed on Russia and Belarus are based on a multilateral approach. More than thirty countries, including major chip producers, such as the European Union (EU), Japan, Singapore, South Korea, and Taiwan, are actively imposing export controls in response to the conflict in Ukraine. The grave threat that Russia's actions in Ukraine pose to global security and economic stability has prompted countries to coordinate with the United States, which is a departure from the approach in the Huawei case, when the United States imposed export controls unilaterally. As a result of this unprecedented, allied cooperation, the U.S. Department of Commerce is exempting countries that adopt similar controls from U.S. FDP rules.

The full effects of the new export controls on Russia, which are part of a broader set of punitive economic measures, are yet to be seen. However, they are already generating blowback. Putin has threatened to issue sanctions on critical minerals, including those needed to produce semiconductors—a move that would significantly impact U.S. military equipment manufacturing, in particular. Chipmakers around the world have tried to diversify their supply chains, but Russia and Ukraine remain key players in the global supply chain. Russia controls approximately 43 percent of global palladium production, and Ukraine supplies approximately 70 percent of the world's neon gas, including 80 to 90 percent of all U.S. imports, both of which are an essential components in chip manufacturing. In 2014, Russia's annexation of Crimea caused neon prices to skyrocket by 600 percent. Although chip companies predict that the industry will face little immediate disruption from Russia's invasion of Ukraine, the cascading impacts of deteriorating U.S.-Russia trade relations and a potential trade war would have far-reaching implications beyond semiconductors.

Countries accelerate indigenization efforts as supply chain disruptions worsen

Heightened concerns of limited access to essential chips, slowed economic growth, and the potential for further damage to already-strained global supply chains make it likely that countries globally will accelerate their chip indigenization strategies and make long-term investments in alternative supply chains. Indeed, the recent export control measures targeting Russia, and concomitant trade disruptions carry cascading impacts for industrial sectors—notably in Europe. The EU is Russia's largest trading partner, and Russia is the EU's fifth largest trading partner, with their total trade amounting to 174.3 billion euros (USD 197.1 billion).

In early February 2022, the European Commission proposed a suite of regulatory changes through the European Chips Act. The Act proposes 43 billion euros ($49 billion) worth of investment to increase chip production across Europe (a figure that attempts to rival the $52 billion funding levels proposed in the United

States) and is part of a broader, more ambitious effort by the EU to quadruple its current global semiconductor output from 5 percent to 20 percent by 2030. While the Act still requires approval from the European Parliament and member states, it demonstrates countries' mounting concerns regarding their dependence on others for access to essential products and services. Beyond Europe, Japan, South Korea, and Taiwan have announced similar plans to boost domestic chip and semiconductor manufacturing equipment production and deepen their economic ties with allies and partners to strengthen supply chain resiliency.

The flux in the chip global supply chain and heightened concerns of China's potential response in the Taiwan Strait following Russia's military incursion in Ukraine may incentivize Taiwan to seek stronger economic and diplomatic ties with key Western countries. In 2021, the world's largest chip manufacturer, Taiwan Semiconductor Manufacturing Company (TSMC), announced plans to invest $100 billion over the next three years to expand its production capacity, which could include fabrication facilities ("fabs") outside of the Asia region. TSMC has expressed interest in establishing its first European fab in Germany, which is a key player in supplying top-of-the-line lasers for chip manufacturing. Although the EU has no official diplomatic ties with Taiwan, Taiwan is the EU's fifteenth largest trading partner and the EU is Taiwan's fourth largest trading partner, with their bilateral trade totaling over $35 billion in 2020. Taiwan may continue to leverage its current position in the global supply chain with respect to semiconductors, and more broadly, to strengthen its ties with Europe to counter Chinese pressure.

Even if the crisis in Ukraine accelerates indigenization efforts, it will take years for countries to expand manufacturing capacity, shore up the necessary talent, and solidify the competitiveness of firms in the chip industry. It is highly unlikely that countries will be able to replicate the complex global ecosystem domestically given that American, Chinese, European, South Korean, Japanese, and Taiwanese firms will remain the primary suppliers of distinct technology and materials that others in the semiconductor supply chain rely upon. Thus, an allied strategy is needed.

The unintended consequences of export controls and economic statecraft

Due to the highly interconnected nature of the global supply chain, U.S. export controls on semiconductors could also have a range of unintended consequences.

GRAPHIC SOURCES: INDUSTRIAL R&D INVESTMENT SCOREBOARD, IC INSIGHTS, INFORMATION NETWORK, MARKETWATCH, MARKET RESEARCH REPORTS, PR NEWSWIRE, SCIENCEDIRECT, SEEKING ALPHA, SEMICONDUCTOR INDUSTRY ASSOCIATION, SOURCE TODAY, TRENDFORCE, AND THE UNITED STATES GEOLOGICAL SURVEY

The Global Path of a Semiconductor

This graphic portrays the complexity of the semiconductor industry ecosystem and emphasizes the necessity to secure each segment individually according to its unique characteristics.

STEP 1

Raw Material Sourcing

Key Countries: Bhutan, Brazil, Canada, China, France, Iceland, India, Malaysia, Norway, Poland, Russia, Spain, Ukraine, United States, and other countries

Semiconductors are usually composed of silicon or gallium arsenide. Each material has advantages depending on the chip's functionality, differing on cost-to-performance ratios, high-speed operations, high-temperature tolerance, or desired response to a signal.

STEP 2

Research & Development (R&D)

Key Countries: China, Europe, Japan, South Korea, Taiwan, United States

Semiconductors make up the greatest percentage of total R&D spending in the world at 23%.

STEP 3

Designing

Key Countries: Taiwan, United Kingdom, United States

Increasing demand for faster technology is driving "fabless" market growth. Fabless firms have no manufacturing capabilities and specifically design chips.

STEP 4

Manufacturing

Key Countries: Germany, Japan, Netherlands,United States, and other countries

Silicon blocks are cut into wafers, circuit partners are printed onto wafers to make microelectronic devices, and finished wafers are sorted and cut into dies.

STEP 5

Assembly, Testing, and Packaging (ATP)

Key Countries: China, Singapore, Taiwan, United States

Chips prepared for shipment. This stage is the most labor-intensive and requires fewer technical skills. It is often performed where wages are comparatively low.

STEP 6

Distribution

Key Countries: China, North America, Singapore, Taiwan

Finished products are shipped to distributors or directly sold to equipment manufacturers. Logistics, both inbound and outbound, are playing an increasingly important role for product launches and customer visibility into the supply chain.

STEP 7

Sales

Key Countries: China, Germany, Japan, South Korea, Switzerland, Taiwan, United States.

Customers buy the end product from the manufacturer.

First, manufacturers are increasingly finding themselves caught in the crosshairs of intensifying geopolitical competition, being forced to choose sides to avoid retaliation. For example, China's anti-foreign sanctions law passed in June 2021, subjects companies doing business in China to penalties should they abide by U.S., EU, and other foreign governments' sanctions. This leaves firms at higher risk of being targeted by Chinese authorities. Similarly, the Biden administration has stated that if companies are found to be violating current export controls on Russia, they will be put on the U.S. Department of Commerce's Entity List.

Second, while export controls on semiconductors are a powerful tool, they could also drive closer Sino-Russo strategic cooperation. Both strategic competitors with the U.S., in February 2022, China and Russia issued a joint statement that outlined their plans for broader economic and technological "friendship." Indeed, China is Russia's largest trading partner, with their trade growing from $10.7 billion in 2001 to $140 billion in 2021. One of the main drivers of Sino-Russo cooperation is Russia's need for technology and capital that China can provide in exchange for natural resources from Russia's enormous reserves. Meanwhile, Putin may look to leverage Russia's influence over the abundance of Arctic natural gas and energy reserves to deepen its connections with China. Experts also warn that in response to the sanctions, Russia may deepen its non-dollar-denominated trade ties and seek support from China in order to evade U.S. sanctions—a move that could in the long run undermine U.S. dominance in the international financial system.

Intensifying Western sanctions on Russia stands to strengthen Russia-China economic and tech partnerships, particularly given that Russia already purchases 70 percent of its chips from China. While China is weighing the degree to which it will support Russia in Ukraine, given the threat of potential secondary sanctions, the Biden administration's actions on export controls and semiconductors may ultimately be constrained by potential opposition from domestic tech companies. The U.S. tech industry is highly dependent on revenue and global supply chains that flow through China. About 80 percent of U.S. firms' export revenue comes from abroad, 36 percent of which is from China. Export revenue is essential for companies' ability to reinvest in vital research and development initiatives that allow U.S. firms to remain at the cutting edge of their sectors.

Looking Ahead

As tensions in Ukraine escalate, the EU-U.S. Trade and Technology Council (TTC), established in June 2021, has a greater role to play in harmonizing allies' approach to mitigating and managing consequences from their sanctions package. While the TCC is currently focused on short-term supply chain issues, the Council's meeting in 2022 will be one to watch to see if the United States and its allies can coordinate a mid- to long-term strategy with respect to semiconductors. Experts warn that current export controls on semiconductors could widen to advanced, commercial chips that do not have specific military applications, but offer high-tech capabilities in critical emerging technology sectors. Such a move would escalate the already broad category of items covered in the current export controls to include, for example, graphic-processing chips used in artificial intelligence (AI), amounting to a near blockade of any key technologies that Russia would rely on.

To learn more about semiconductors and intensifying geostrategic competition, see FP Analytics' Semiconductor and the U.S.-China Innovation Race special report, which examines the interconnectivity and fragility of global supply chains and the central role of Taiwan in global tech competition.

For a comprehensive breakdown of the key factors determining the future of 5G technology and infrastructure, see FP Analytics' 5G Explained Power Map. ■

PUBLISHED ON MARCH 8, 2022

What Does Russia's Removal From SWIFT Mean for the Future of Global Commerce?

Removing Russian banks from the SWIFT system is accelerating a global economic realignment.

A police officer walks past the offices of the Russian Central Bank in Moscow on Feb. 28.
MIKHAIL TERESHCHENKO/ TASS VIA GETTY IMAGES

By **Christian Perez**,
Senior Policy & Quantitative Analyst with FP Analytics

With the rapid escalation of Russia's invasion of Ukraine, a large coalition of states, including the EU, U.S., Canada, and the UK, among others, agreed on February 26th, 2022, to ban select Russian banks from the Society for Worldwide Interbank Financial Telecommunications (SWIFT) international payment messaging system. The move was the latest in a series of severe sanctions aimed at economically isolating Russia and crippling the Russian financial system in order to pressure the Putin regime to end its military operations in Ukraine.

Seven Russian banks were removed from SWIFT, effectively denying them access to international markets. However, the list of those targeted did not include Sberbank or Gazprombank, two of Russia's largest banks by assets. The decision to impose a selective ban is primarily due to Europe's continued reliance on Russia for energy, and concerns that removing all Russian banks would create further turmoil in global energy markets. Removing the selected Russian banks from SWIFT is already having a discernible negative impact on Russia's economy, but determining the long-term impact is more complicated. Russia is intricately connected to the global economy, holds large quantities of critical resources, and has been strategically preparing to weather the long-term impacts of sanctions and a removal from SWIFT since 2014, when Putin annexed Crimea.

The global role of SWIFT, the implications of Russia's removal, and the potential long-term impacts it will have on the global economy are broken down below.

Understanding how the SWIFT system facilitates global financial transactions

A consortium of U.S. and European banks created the SWIFT system in 1973 to facilitate the exchange of interbank messages containing the secure payment

and transfer information for settling international transactions. Today, SWIFT is the most widely used interbank messaging system in the world, with over 11,000 member banks and financial institutions in over 200 countries and territories. Based in Belgium, SWIFT is jointly owned by more than 2,000 banks and financial institutions and is overseen by the National Bank of Belgium, in partnership other major central banks, including the U.S. Federal Reserve and the Bank of England. In 2021, the SWIFT platform processed more than 10 billion messages and facilitated trillions of dollars in cross-border payments. Roughly one percent of these payment messages were linked to Russia.

Critically, SWIFT does not actually move or hold money or securities, nor does it function as a clearinghouse for settling transactions between banks. SWIFT's main function is to enable banks to communicate transaction information, thereby facilitating payments for imports and exports. Although several Russian banks are now cut off from SWIFT, they can still execute international transactions with other banks. However, in lieu of SWIFT, they must use slower and less-secure methods of interbank communication, such as the outdated telex telegram network or phone calls and email.

In 2014, the U.S. and EU threatened to cut Russian access to SWIFT as part of the sanctions package they imposed after Russia's annexation of Crimea. In response, Russia developed its own internal financial transaction messaging system, the System for Transfer of Financial Messages (SPFS), aimed at reducing its reliance on SWIFT. Today, the SPFS system is used as the primary messaging system in 20 percent of Russia's domestic transactions, and its banking network includes 23 foreign banks. The SPFS is not as technically advanced as SWIFT, but it is widely used domestically and could serve as a functional alternative to execute foreign transactions.

Russian capacity to adjust to SWIFT removal is severely limited by additional Western sanctions

The removal of Russian banks from SWIFT, coupled with the other extensive Western sanctions being levied, has the potential to fundamentally restructure the Russian economy. In 2012, Iran lost nearly half its oil revenues and saw a 30 percent decline in foreign trade after being removed from the SWIFT system for ramping up its nuclear program. Additionally, in 2014, when the U.S. and EU initially threatened to disconnect Russia from SWIFT, Russia's finance minister estimated that the move would lead to a 5 percent drop in Russian GDP. Two of Russia's three largest banks are still connected to SWIFT, even if they were to be banned later, there are alternative methods for interacting internationally without reliance on SWIFT. Nevertheless, Russia's

International Funds Transfer Using the SWIFT System

Countries and industries rely on intermediary institutions such as SWIFT to communicate the necessary financial instructions, without which they cannot transfer money or settle payments across borders. SWIFT's global payments platform handles $77 trillion in cross-border transactions, accounting for 56 percent of the global total. When a bank has branches in multiple countries, SWIFT transfers the settlement instructions between banks, and the receiving bank can execute the transaction settlement internally.

Example of International Payment Using SWIFT

STEP 1
An executive in Country A instructs his bank to pay an aluminum company in Country B for imported materials.

STEP 2
The Country A-based bank branch sends a message through SWIFT to its Country B-based branch.

STEP 3
The Country B-based bank branch receives the SWIFT message with payment instructions.

STEP 4
The Country B-based bank settles the transaction and credits the aluminum company's account.

SOURCE: U.S. DEPARTMENT OF THE TREASURY—FINANCIAL CRIMES ENFORCEMENT NETWORK

economy is set to suffer severe setbacks.

In 2014, Western sanctions caused the value of the ruble to drop by over 50 percent against the dollar and led to a sustained decline in GDP growth over the next two years. Russia has since attempted to further sanction-proof its economy, through building up $600 billion in foreign reserves, diversifying those reserves to include more euros and renminbi, reducing the national debt, and limiting imports of some goods. Despite these efforts, Russia is still heavily reliant on the dollar system and Western markets. At the end of 2021, 16 percent of Russia's foreign reserves were held in dollars, and 32 percent in euros, while Germany, the Netherlands, and the U.S. were all among its top trade partners. With these countries now enforcing strict sanctions, Russia's economy is in a precarious position—one that is causing ripple effects across global markets including supply chain disruptions and higher prices on energy and agricultural goods.

U.S. sanctions against Russia will be particularly impactful, as the majority of global trade is conducted in dollars, and the U.S. can freeze any dollar transactions before they are settled. Since the U.S. sanctions went into effect, the value of the ruble has dropped nearly 30 percent against the dollar, and Russian bond prices have plummeted as investors fear they will be unable to meet outstanding debt obligations. Global supply chains, already stressed from the fallout of the COVID-19 pandemic, are now under further pressure. Russia is a key exporter of oil and gas, the world's largest producer of palladium and the second-largest producer of platinum—key commodities used in semiconductor manufacturing—and a major exporter of other critical minerals, mining commodities, and agricultural goods. Limiting Russian exports has led to price spikes in these commodities globally, but with limited alternative suppliers it is likely that Russia will soon be able to find willing trade partners across Asia, Africa, and the Middle East.

Countries such as China, India, and Turkey have all signaled their initial willingness to continue doing business with Russia—potentially accelerating a global economic divide between Western-aligned and Russian-aligned economies. These countries will still need to contend with the limitations on trade from sanctions and the SWIFT ban, in addition to the of risk exposing themselves to secondary sanctions as a result of doing business with Russia. However, Russia's abundant resource reserves, and a desire to break away from the current U.S.-dominated financial system, could drive them to continue economic relations with Russia and move further away from the West.

Russian banks' removal from SWIFT will further contribute to global reorientation of economic relationships

With no clear end in sight, Russia's invasion of Ukraine is already accelerating a broad global economic reorientation. Europe is set to shift away from its reliance on Russian oil and gas, while Russia will be forced to rely primarily on non-Western-aligned nations for trade markets for the foreseeable future. Mirroring

SWIFT Alternatives

Russia and China have developed domestic alternatives to the SWIFT system.

RUSSIA

System for Transfer of Financial Messages (SPFS)

404 financial institutions connected to SPFS, including 23 banks in Armenia, Belarus, Germany, Kazakhstan, Kyrgyzstan, and Switzerland.

13 million messages per year, accounting for 20 percent of domestic transactions, in 2021.

CHINA

Cross-Border Interbank Payments System (CIPS)

Designed to supplement 15 renminbi offshore clearing centers (in addition to Hong Kong and Macau), along with the overseas branches of the major state-owned commercial banks (ICBC, BOC, and CCB).

Processed around 80 trillion renminbi ($12.68 trillion), or roughly 220 billion renminbi per day, in 2021.

SOURCES: BROOKINGS, REUTERS, FEDERATION OF AMERICAN SCIENTISTS, RUSSIAN COUNCIL, NSPK

Russia's efforts to sanction-proof its economy, China has been working to create an alternative financial system beyond the reach of U.S. and EU sanctions. In 2015, China began developing its own alternative to SWIFT, the Cross-Border Interbank Payment System (CIPS). While adoption of CIPS has been slow, in 2021 CIPS processed around 80 trillion renminbi ($12.68 trillion) in transactions, a 75 percent increase from 2020, and now has 1,280 financial institutions in 103 countries and regions connected to the system. China has been promoting the international use of the renminbi as an alternative to the dollar with limited success since the 2008 financial crisis, but removing Russian banks from SWIFT could provide an opening for China to significantly expand the use of both the CIPS and the renminbi in international trade.

The extent to which China is willing to bring Russia into its economic sphere is still unclear, especially as the war in Ukraine drags on. China's foreign ministry initially condemned Western sanctions on Russia and announced that it will continue normal trade relations. Russia is a major provider of key resources that are critical to China's long-term development plans, including energy supplies and critical minerals used in semiconductor manufacturing, as well as rapidly opening trade routes through the Arctic. During the Beijing Olympics in early 2022, China and Russia agreed in principle to boost bilateral trade to $250 billion by 2024, and trade between the two countries has grown to its highest level ever since the start of 2021. Amidst deteriorating relations with the U.S., it is unlikely that China will reject the chance to increase its access to Russian resources and expand its sphere of economic influence.

India has also been increasingly turning to Russia for energy supplies and is now exploring setting up rupee-based trade accounts with Russia. Additionally, Russia has been working on extending its Eurasian Economic Union (EEU) free-trade zone, which grew to include Vietnam in 2015 in addition to existing members Russia, Armenia, Belarus, Kazakhstan, and Kyrgyzstan. As Western sanctions take effect, Russia will become largely isolated from U.S. and EU markets, but its large reserve of natural resources and strong ties to China and central Asia decrease the likelihood that it will become as economically isolated as countries like North Korea or Venezuela. Instead, if the conflict in Ukraine continues, and Western sanctions persist, economic relations with Russia could help accelerate the growth of a non-Western bloc in the global economy.

To help understand the full scope of this coming evolution, FP Analytics' Future of Money Power Map series breaks down China and Russia's threats to the existing dollar system, the coming impact of technology, and the key challenges that governments, businesses, and individuals need to be prepared to navigate. ■

PUBLISHED ON FEBRUARY 25, 2022

How Russia's Future with NATO Will Impact the Arctic

Three critical ways the crisis in Ukraine will determine the region's future.

A soldier holds a machine gun as he patrols the Russian northern military base on Kotelny island, beyond the Arctic circle on April 3, 2019. The Russian military base is home to 250 soldiers and is to serve as a model for future military installations in the Arctic.
MAXIME POPOV /AFP VIA GETTY

By **Christian Perez**,
Senior Policy & Quantitative Analyst with FP Analytics

The geopolitical importance of the Arctic region is coming back into focus as Russian troops further encroach into Ukraine. The Russian invasion is further deteriorating relations and highlighting critical fault lines between Russia and NATO-allied states. In determining their response to Russian aggression, NATO allies are weighing key considerations, including the various impacts from the potential use of force, balancing the use of sanctions with Europe's reliance on Russian energy supplies, and addressing Russia's strengthening ties with China.

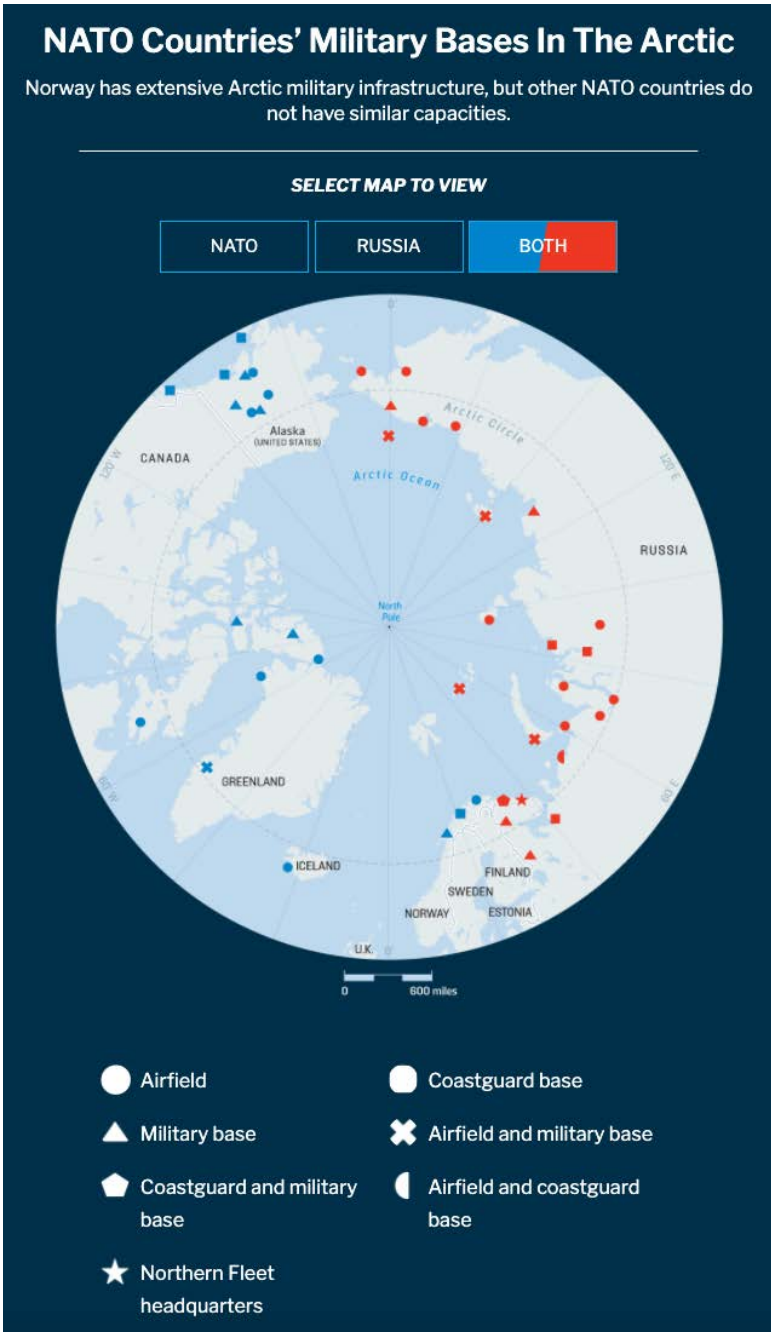
The Arctic region is set to play a key role in each of these considerations. Abundant natural gas and energy reserves are concentrated in Russian Arctic territory, which European countries are highly dependent on for their energy supply. Meanwhile, Russia has made the Arctic a focal point of its military modernization efforts, leading to a steady buildup of Russian and NATO forces throughout the region. The widespread military buildup since 2007 amplifies the potential for a conflict between Russia and NATO-allied states to spill over into the region. Armed conflict in the Arctic could permanently damage regional cooperation, compromising coordinated efforts, dating back to 1996, among the Arctic states (Canada, Denmark, Finland, Iceland, Norway, Russia, Sweden, and the U.S.) in search-and-rescue operations, environmental protection, and prevention of illegal fishing, among other issues. President Putin is also leveraging Arctic resources to strengthen his hand elsewhere, including deepening connections with China by announcing renewed cooperation in the Arctic and signing a new 30-year agreement on energy exports in early February. As the Ukraine crisis evolves, the Arctic's role and the impact the crisis could have on the region are broken down below.

Armed conflict threatens longstanding Arctic cooperation

Today, the Arctic is the only region where Russia has military and strategic supremacy, and as the ongoing crisis in Ukraine escalates, it brings with it increased risk for conflict in the Arctic. Since 2014, Russia has built over 475 new structures across its Arctic military strongholds and has conducted extensive military exercises, most recently in January 2022. Both Russian and NATO troops are currently stationed in close proximity throughout the region and have conducted war games in the same geographic vicinities, such as the Norwegian Sea. As the situation along the Ukrainian border escalates tensions between NATO allies and Russia, the fallout from a miscalculation across a militarized Arctic could become severe.

Since Russia's 2014 annexation of Crimea, the Arctic has served as one of the key arenas in which cooperation among the U.S., Russia, and other Arctic nations has continued to progress. However, an escalation of the Ukraine conflict could limit communication between Russia, the U.S. and other Arctic states and undercut coordination on common regional interests. Additionally, a breakdown in communication between Russia and other Arctic nations would further heighten the risk of a miscommunication between Russian and NATO forces stationed across the region.

The emergence of a conflict would risk not only ending cooperation in key areas across the Arctic, but also potentially fraying the Arctic's existing patchwork governance structure. Arctic governance, as currently constructed, consists of various national standards, laws, and treaties, with the Arctic Council serving as the most comprehensive governance forum. These forums have played a critical role in improving relations between Russia and NATO-allied states in the past—for example, after the Russo-Georgian war in 2008, cooperation in the Arctic helped normalize relations between Russia and the other Arctic states. In contrast, the former Arctic Chiefs of Defense Forum, the main venue for security dialogues with Russia in the Arctic, was suspended in 2014 after Russia's annexation of Crimea. The remaining governance structures are meant to facilitate cooperation among Arctic nations and indigenous groups on small-scale regional issues, not contain great power competition or resolve armed conflicts. An escalation of the current crisis in Ukraine will provide a major test for Arctic governance structures and determine, in part, the extent of future coordination with Russia across the region.



SOURCES: MILITARYBASES.COM, GLOBALSECURITY.ORG, CANADIAN GLOBAL AFFAIRS INSTITUTE DECEMBER 2020

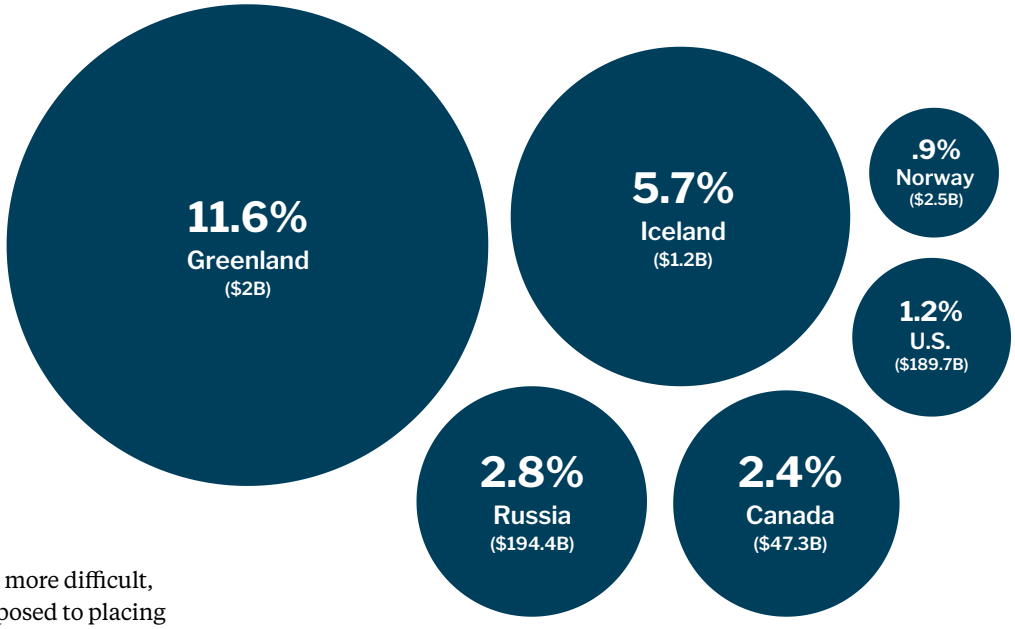
Europe's reliance on Russian energy limits sanctions' effectiveness

As Russia amassed some 200,000 troops along the Ukrainian border, European countries have faced record-high increases in natural gas prices and a regional energy crisis exacerbated by Europe's longstanding reliance on Russian energy supplies. Despite its efforts to diversify its energy mix, Russia remains the EU's single largest energy source, supplying roughly a third of Europe's natural gas and a quarter of its crude oil. The Arctic is estimated to contain roughly 13 percent of the world's oil reserves, and nearly 30 percent of its natural gas reserves, much of which resides in Russian territory. Russia is already the world's third-largest producer of oil and second-largest producer of natural gas, and Russian energy exports play a critical role in supporting Europe's power supply. This relationship between Europe and Russia has made

Chinese Investment in the Arctic

A large influx of Chinese FDI accounted for a significant portion of Iceland and Greenland's total economic output from 2012 to 2017.

PERCENTAGE OF GDP (TOTAL U.S. DOLLARS)



SOURCE: CNA ANALYSIS AND SOLUTIONS

enforcing effective sanctions on Russia more difficult, as many European states have been opposed to placing sanctions on Russia's energy sector—the most important part of its economy. However, the crisis in Ukraine is rapidly changing this assessment, potentially altering Europe and Russia's future economic relationship.

The Nordstream 2 pipeline has played a central role in the debate over Russian sanctions. In September 2021, the Russian company Gazprom completed the pipeline, which would enable Russia to funnel natural gas directly from Russia to Germany, effectively doubling its capacity to export natural gas to Europe. The pipeline would also allow Russia to circumvent Ukraine and export natural gas directly to EU states, severely limiting Ukraine's leverage, as numerous existing natural gas pipelines that Russia uses run through Ukrainian territory. However, the pipeline has never been operational, due to pushback from the U.S. and other European countries. Germany has now halted its certification after Russia recognized the independence of two separatist regions in eastern Ukraine (the Donetsk People's Republic and the Lohansk People's Republic) on February 22nd and began mobilizing troops into Ukraine's Donbas region, where they are located. With further sanctions coming after Russian airstrikes in Ukraine, Russia's energy sector could be targeted with additional restrictions.

This development signals a significant shift in the EU's approach, but also leaves it vulnerable to Russian retaliation. Russia could further limit its energy exports to Europe, forcing countries in the region to seek alternative suppliers from the U.S. and Middle East and elevating already near-record-high energy prices. While the loss of sales to the EU market would hurt Russian export revenue in the short term, Russia has been securing new energy export customers in Asia. China has been particularly eager to purchase Russian energy supplies, which could help sustain Russia's energy sector in the face of additional EU and U.S. sanctions.

Deepening ties with Russia could expand China's Arctic influence

Closer cooperation with Russia grants China the chance to expand its role in the Arctic, where it has been steadily ramping up its activity over the past decade, further transforming the region into a future arena of great power competition. In 2013, China became an Arctic Observer state on the Arctic Council, and from 2012 to 2017 it invested over $435 billion across Arctic states in a range of sectors, including research, infrastructure, and resource extraction. In 2018, China published its Arctic Strategy and outlined its plan for a "Polar Silk Road" as part of its Belt and Road Initiative. China's interest in the Arctic to date has centered on ensuring access to the rapidly opening Northern Sea Route—an Arctic shipping lane connecting Europe and Asia along Russia's Northern ocean—and securing a share of the region's energy and critical mineral reserves. Pursuing these interests has led to major economic agreements with Russia, including a $400 billion natural gas deal signed in 2014 and, most

recently, a 30-year natural gas deal finalized this month.

China and Russia's cooperation in the Arctic is sparking further security concerns from the U.S. and EU and is generating speculation that China is using the Arctic as an arena to expand its global ambitions. While Russia can supply China with energy resources, China provides a lucrative market for energy exports, access to capital, and financial services to counteract NATO sanctions on Russia. Additionally, China's participation in Russian military drills, conducted in the Arctic in 2018 and 2019, raises concerns that future agreements between the two nations in the region could include military cooperation. As the ongoing crisis in Ukraine leads to new sanctions on Russia from both the U.S. and EU, it is likely that Russia will increasingly turn to China for economic support. While that bilateral relationship is nuanced, this dynamic could create an opening for China to further pursue and cement its long-term presence in the Arctic region. An expansion of China's role in the Arctic would increase tensions with the U.S. and other Arctic nations already wary of China's intentions, and potentially catalyze a transformation of the Arctic's future role in geopolitics.

Looking Ahead

As Russia continues its invasion of Ukraine and challenges NATO, the Arctic is positioned to play a crucial and growing role in future geopolitical, economic, and military affairs. The abundant resources contained in the Arctic, combined with Russia's strong military position in the region, are rapidly becoming critical factors in determining the U.S. and EU's strategic engagement with Russia. For a deeper dive, FP Analytics' Arctic Competition Power Map breaks down the varying dimensions of Arctic resource and military competition, and comprehensively lays out the interests and strengths of each Arctic nation. ■

PUBLISHED ON FEBRUARY 14, 2022

Is It Time for the U.S. to Issue a Digital Dollar?

Crucial foreign-policy questions need to be answered first.

Federal Reserve Board Chairman Jerome Powell speaks during a news conference in Washington, D.C. on January 29, 2020.
SAMUEL CORUM/GETTY IMAGES

By **Christian Perez**,
Senior Policy & Quantitative Analyst with FP Analytics

By **Gahyun Helen You**,
Policy Analyst with FP Analytics

Amid increased interest from Congress in cryptocurrencies and stablecoins, in late January 2022, the U.S. Federal Reserve published its discussion paper on central bank digital currencies (CBDCs). Based on the paper, it appears that while the Fed recognizes the potential benefits CBDCs can have on payment systems—from financial inclusion to maintaining the dollar's primacy in the global economy—it has more questions than answers regarding key policy concerns about monetary and financial stability risks, and the potential impacts a U.S.-issued CBDC would have on the global financial system.

Currently, 87 countries representing 90 percent of global GDP are exploring a CBDC. Of the four largest central banks in the world (the Euro Zone, Japan, the United Kingdom, and the United States), the United States is the furthest behind in CBDC development due to privacy concerns, regulatory hurdles, and divisions within Congress on whether a U.S.-issued CBDC is necessary. While U.S. financial institutions understand the need to address gaps in the current financial system—as demonstrated by the Fed's plans to launch its FedNow Service in 2023, which seeks to provide instant payment services for interbank settlements—heightened interest in CBDCs, particularly from China and Russia, is prompting the Fed and other central banks around the world to explore and evaluate their potential roles in the digital asset ecosystem.

In an effort to address these important issues, we tackle five key foreign policy questions posed by the Fed in its discussion paper and highlight related issues that warrant further attention.

1. Could some or all of the potential benefits of a CBDC be better achieved in a different way?

There are many payment technologies currently in use or under development that could replicate the benefits of a CBDC on a domestic level. For example, technologies such as real-time gross settlement, new forms of non-cash payments, and real-time payments can replicate some of the potential benefits of CBDCs or stablecoins in the payments space. From an inclusion perspective, globally, there are numerous fintech companies dedicated to expanding access to financial services around the world, such as Akaboxi in Uganda and Teknospire in India, in addition to numerous U.S. start-ups. These companies provide access to banking services in underserved communities and lower the costs of remittances potentially as effectively as a CBDC.

Internationally, there are potential benefits of a U.S. CBDC that may be harder to achieve via other means. The main benefits would come from the widespread use of a U.S. CBDC to maintain the dollar's importance in the international payments system by securing a dominant position in the future of international payments architecture and countering foreign countries' active attempts to gain influence. For example, the Society for Worldwide Interbank Financial Telecommunications (SWIFT), which is critical for conducting cross-border financial transactions, is already exploring working with China's digital renminbi. This could facilitate China's shift away from its reliance on the dollar and move it closer to eventually providing a viable alternative to the existing dollar-centric system. Such a shift would erode the United States' global economic standing and limit its international influence by providing an alternative financial system beyond the reach of U.S. sanctions.

In the short term, it is highly unlikely that the dollar's dominant international role will be usurped. At least 60 percent of exports are invoiced in dollars in Latin America, Sub-Saharan Africa, Central Asia, East and Southeast Asia, and the Pacific, according to the International Monetary Fund (IMF), with the remainder divided between local currencies and the euro. At present, the renminbi is not poised to challenge the dollar's role as the world's reserve currency, given that it is not freely exchangeable and Chinese capital account is closed.

The United States cannot take its primacy for granted, however, and must dedicate resources establish the necessary digital infrastructure to facilitate and meet the rising demand for faster, more secure, and cheaper electronic forms of payment, especially if the United States seeks to retain and incentivize consumers, businesses, and markets to function within a U.S.-led financial system. To date, nine countries have launched their own CBDC—the most recent being Nigeria's eNaira in October 2021—and as China and Russia pilot their digital currencies and build alternative financial infrastructures, the United States must address the inefficiencies of the current payment systems, particularly for cross-border transactions in emerging market economies; otherwise, it risks losing its influence within the global financial system. Processes to watch in the coming months include the Central Bank of Russia's test of digital ruble transactions across a dozen commercial banks, including ones located in the illegally annexed region of Crimea. China is similarly piloting its digital yuan at the Winter Olympics—the first time the e-CNY is being made available to foreigners.

2. How should decisions by large-economy nations to issue CBDCs influence the decision of whether the U.S. should do so?

The United States should bear in mind the varying reasons that other countries are issuing CBDCs and move forward with a clear understanding of the purpose(s) a digital dollar would aim to achieve. Some smaller countries have released CBDCs for consumer use, which has focused expressly on increasing financial inclusion, such as the Bahamas' Sand Dollar. While this could be one benefit of a U.S. CBDC— 5 percent of U.S. households lack access to a bank account—most large-economy nations have focused on broader policy goals. China's recently issued CBDC is being used to undercut the influence of private payment providers like Alipay, provide data on citizens' economic activity, and potentially push forward the process of internationalizing the renminbi. A U.S. CBDC following this model would generate serious privacy concerns and raise questions about undercutting domestic private-sector innovation. Countries like Russia and Iran are using CBDCs as a way to evade U.S. sanctions and limit the use of native cryptocurrencies like Bitcoin. Using a U.S. CBDC to limit the effectiveness of sanctions-evasion efforts is possible, in theory, by working with existing international financial institutions to adopt a U.S. CBDC and limit the adoption of foreign alternatives. However, as things stand today, the United States is a ways away from both the technical capacity and the government consensus necessary to move forward with such a strategy.

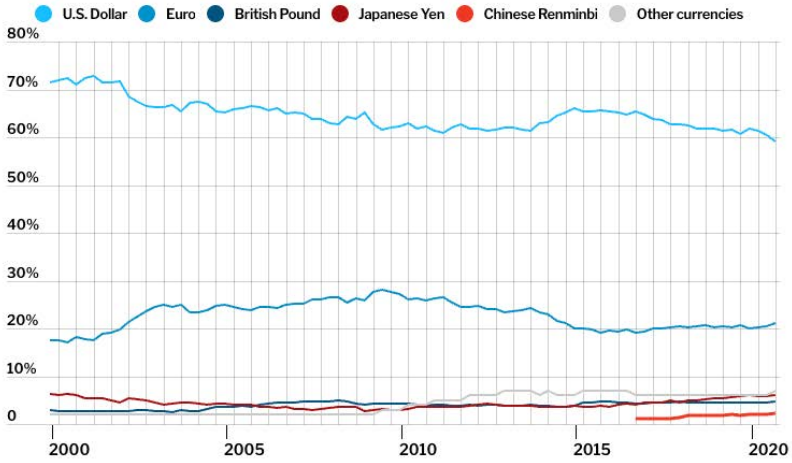
While CBDCs are a significant development in international finance, the United States should not be looking at other nations issuing CBDCs in isolation. Both China and Russia have developed alternatives to the SWIFT system and are moving toward de-dollarizing their foreign exchange reserves in an effort to decrease their economic reliance on the dollar and weaken

the impact of U.S. sanctions. In order to determine appropriate next steps, the U.S. should be closely watching not just CBDC development, but also efforts to internationalize their use and the impact that such efforts could have on governments' influence abroad and on the global financial system. For example, China's partnership with SWIFT to globalize its digital renminbi, or the potential issuance of loans denominated in digital renminbi to other countries, pose more significant challenges to U.S. interests internationally than the domestic launch of its digital currency alone.

Key considerations must also be given to how countries are designing their CBDCs and digitizing their financial services. As countries roll out their digital currencies, differing data, privacy, and messaging standards pose significant interoperability challenges, which could hinder funding flows among CBDC payment systems. The United States' limited progress in its CBDC program may require it to adopt technical features from other countries so that it can be complementary to its allies who, in some cases, are already piloting their CBDCs. For example, South Korea finished its first test phase for a digital won in January 2022 and is now entering its second research phase. Japan similarly plans to distribute its digital currency called DCJPY, which seeks to improve large-scale fund transfers and settlements among companies in 2022. And while the European Central Bank's (ECB) digital euro is in the early experimenting phases, the ECB plans to begin working on a prototype by the end of 2023. Further international collaboration on CBDC standards is needed to ensure interoperability and minimize disruptions in financial flows.

Global Foreign Reserves Composition

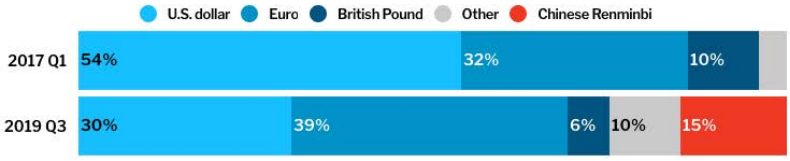
Since 2000, the share of global reserves held in U.S. dollars has steadily declined, from over 70 percent in the earily 2000s to 59 percent in Q4 2020.



SOURCE: INTERNATIONAL MONETARY FUND

Composition of Russia's International Reserves

In response to 2018 sanctions from the Trump administration, Russia cut its share of dollar reserves and increased its euro and renminbi holdings.



SOURCE: CENTRAL BANK OF RUSSIA

3. Could a CBDC adversely affect the financial sector? How might a CBDC's effect on the financial sector differ from that of stablecoins or other non-bank money?

Early Design Considerations Will Determine the Ultimate Impacts of a U.S. CBDC. The impacts that a U.S. CBDC could have on the financial sector largely depend on the design ideas embedded into the technology. Absent from the Fed's paper was a discussion of the differences inherent in retail versus wholesale CBDCs, and a clarification of which options are being considered. The risks, benefits, and design considerations will all vary, depending on whether the United States issues a retail CBDC, a wholesale CBDC, or both, and this should be one of the first decisions made before moving forward with developing a digital dollar. Based on the framing of the paper and previous congressional hearings, it appears that most of the debate is about issuing a retail CBDC, which would effectively act as a digital dollar that consumers could use for transactions, similar to the digital renminbi that China is now in the process of testing.

Many of the issues currently being debated by the Fed in relation to privacy, private-sector involvement, cybersecurity risks, and shocks to the financial system relate specifically to issuing a retail CBDC. If the United States were to pursue this route, it would add significantly higher stakes to design considerations. With a retail CBDC, it is possible the Fed could issue CBDC directly to consumers and risk disintermediating parts of the existing banking system while significantly expanding the role of the Fed. To avoid this risk, and to leave the existing financial structure in place, any retail CBDC issued by the Fed would need to leverage existing digital financial service providers and commercial banks for distribution.

In contrast to the retail approach, a wholesale CBDC would use blockchain to improve the efficiency of interbank transactions but would not be issued directly to individuals. A wholesale CBDC model would leave the existing banking system intact and is unlikely to pose serious financial stability risks. Many of the most advanced CBDC projects in developed countries,

such as Project Jasper in Canada and Project Ubin in Singapore, have focused primarily on developing a wholesale CBDC model. The development of a wholesale CBDC would not have the same potential financial inclusion benefits, but it would be an effective approach for developing CBDC technology at lower risk and maintaining the existing importance of the dollar in international transactions.

Addressing Cybersecurity Concerns Must Also Be Prioritized. One of the top concerns briefly raised in the Fed's report, which warrants further consideration, is cybersecurity. Cyberattacks are growing in frequency and sophistication, with experts noting that state-sponsored threat actors are adapting to more robust security in the critical infrastructure by looking for vulnerabilities among financial services, the defense industrial base, NGOs, critical manufacturing, and IT organizations. Indeed, Cybersecurity Ventures estimates that the cost of global cybercrime—which is driven largely by financial gain—will reach $10.5 trillion annually by 2025. In 2021, over $4 billion in cryptocurrencies were stolen by hackers. Depending on how a CBDC is designed and whether it is for retail or wholesale use, the cybersecurity risks will vary. However, as the digital asset ecosystem expands with more actors entering this space, the financial sector will face mounting challenges to address existing and emerging threats (such as those associated with quantum computing, which can compromise data encryption methods) to its security. Given the decentralized nature of the industry, it will likely be difficult to standardize data protection, privacy, and law enforcement data-sharing rules, particularly as countries in Europe and the United States are already struggling to harmonize their cybersecurity frameworks.

Global Status of Key Retail and Wholesale CBDC Projects

Today, domestic banks already have access to electronic central bank money, but transfer is done using a wholesale CBDC would replace the current credit/debit system process with a digital token.

SOURCES: BANK OF ENGLAND, BANK OF CANADA, BANQUE DU FRANCE, MONETARY AUTHORITY OF SINGAPORE, PRICEWATERHOUSECOOPERS, SOUTH AFRICA INTERGOVERNMENTAL FINTECH WORKING GROUP

4. How might domestic and cross-border digital payments evolve in the absence of a U.S. CBDC?

In the absence of any U.S. action, it is likely that cross-border payment systems will continue to integrate more efficient technologies while simultaneously moving away from reliance on the U.S. dollar as their primary currency. The integration of new technologies into the digital payments space is currently driving a transition toward faster and cheaper cross-border payments. For example, SWIFT recently updated its messaging system while new services like Ripple aim to use blockchain for instantaneous international transactions. Alongside technological innovation, intense competition from China, Russia, and, to some extent, the EU and other states, is emerging in efforts to increase influence over international financial architecture. Developing a robust U.S. CBDC could help the United States set international standards, patent key technology, and ensure that the United States keeps pace with technological innovations in the payments space. The United States should not take for granted that the dollar will retain its primacy, particularly if other major geopolitical power shifts continue or if new blockchain-based technologies begin replacing existing cross-border payment systems.

Meanwhile, as the Fed and other central banks around the world explore the possibility of a CBDC, it is highly likely that existing stablecoin issuers and other private-sector entities will seek to expand the adoption of their digital currencies and push for regulations that support the stablecoin sector's long-term growth. Currently, the top stablecoins by market capitalization are backed by the dollar, with companies' projects such as Circle's USD Coin and JP Morgan's JPM Coin looking to provide the speed and convenience of a digital currency with the strength and utility of fiat currencies. Industry leaders have advocated that given the nascent stages of U.S. CBDC development, dollar-backed stablecoins could provide a way for the dollar to maintain its leadership in the global financial system while providing the same benefits as CBDCs. However, stablecoins have their own challenges, namely that they are predominantly used to allow consumers to participate in other digital asset platforms for speculative trading rather than for retail use. As

a result, there are still lingering questions about the roles stablecoins should play in the financial system and whether they would truly serve as an adequate replacement for a U.S. CBDC.

5. How could a CBDC provide privacy to consumers without providing complete anonymity and facilitating illicit financial activity?

The discussion paper suggests that the Fed may be looking to design a CBDC with the following features: 1) pseudonymity to protect user's privacy but not provide anonymous use that could allow for illicit financial activities to occur; 2) intermediation, or hosting, by private banks and financial service providers; and 3) transferability, meaning its value can easily be shared among various intermediaries.

Given the investments in R&D and technology needed, as well as current divisions in the federal government, it is highly unlikely that the United States will issue a digital dollar within the next five years. Depending on how the United States issues its CBDC, should it ultimately do so, there are different approaches to privacy that could be pursued. If the United States decides to issue a retail CBDC, it will need to decide first whether it will use blockchain-based technology or other means. The decision to use blockchain could help address privacy concerns but would invite a slew of additional design considerations. It would need to be decided whether the central bank should be responsible for hosting the underlying physical blockchain infrastructure or whether to run the CBDC on an existing blockchain such as the Ethereum network. In theory, running a CBDC on a decentralized platform, like Ethereum, would provide the highest degree of privacy but would also move some aspects of control over the currency away from the central bank. Considering the issues with hacks, transaction prices, and scalability that have plagued Ethereum and other blockchain networks to date, pursuing this option for a digital dollar would bear considerable risk.

If the United States does ultimately choose to pursue this route and use a public blockchain, it would still need to make upfront decisions about the degree of privacy embedded into its CBDC design. Transactions could be made nearly untraceable and anonymous, or more accessible and transparent than they are today.

The United States could also take a middle-of-the-road approach by making commercial banks and private companies responsible for onboarding consumers and handling privacy elements, such as know your customer (KYC) requirements. This approach would come closest to replicating how the financial system handles consumer privacy today, making government access to personal financial data subject to the existing rules outlined in the Right to Financial Privacy Act. The issue of privacy is likely to continue to be contentious, as China's CBDC has been criticized by some as a tool for the government to surveil its population. Legislation has already been introduced in Congress to curb government oversight of a potential U.S. CBDC largely based on privacy concerns.

During the House Committee on Financial Services hearing in December 2021 regarding stablecoins and cryptocurrencies, industry leaders agreed that all digital currency transactions must be associated with a legally traceable identity in order to prevent and address criminal transactions. In addition to adopting best industry practices, if a U.S.-issued CBDC is pursued, one relatively simple solution that has been proposed is the creation of pseudonymous identification numbers for users, which could be de-anonymized by a federal agency pursuant to a court order. One example would be a randomized tax identification number that would be anonymous to market participants, but their real identities could be stored and managed by a federal agency that would be able to identify who that individual or organization is, if necessary. However, as discussed previously, this brings many data governance questions in addition to privacy issues, especially as differences among China, the European Union, and the United States challenge how businesses and consumers approach international data flows and storage.

Learn More

For a deeper dive into the new technologies and geopolitical tensions driving transformations in the international financial system, FP Analytics' Future of Money Power Map breaks down how the varying systems operate and forces influencing change, and the Global Data Governance Power Map walks through evolving national frameworks focused on managing cross-border data flows and the ongoing challenges to doing business in an increasingly complex regulatory environment. ■

PUBLISHED ON JANUARY 28, 2022

Why China's New Data Security Law Is a Warning for the Future of Data Governance

Stricter data privacy guidelines present new challenges for businesses operating in the world's second largest economy.

Pedestrians walk past a stock market display board showing the Chinese state-owned commercial banking company Bank of China in Hong Kong on Sept. 24, 2020.
BUDRUL CHUKRUT/LIGHTROCKET VIA GETTY IMAGES

By **Christian Perez**,
Senior Policy & Quantitative Analyst with FP Analytics

China's two newest data security laws—the "Data Security Law" (DSL) and the "Personal Information Protection Law" (PIPL)—came into effect at the end of 2021. Building on the 2017 Cybersecurity Law, they include new guidelines for handling data, updated enforcement measures, and additional restrictions on the transfer of data outside of China. Notably, the DSL broadly expands the extraterritorial reach of China's existing data rules, creating a critical new set of guidelines for companies doing business with Chinese citizens—both within and outside the country's borders—to navigate.

These new restrictions paint a complicated picture for the future of data governance, continuing a trend toward more complex regulatory regimes, competing legal frameworks, and increased restrictions on international data flows. Governments continual adoption of similar measures will increasingly disrupt an era of relatively restriction-free cross-border data flows that has been critical to the growth and expansion of many international businesses. The key points and implications from each law are broken down below.

The Data Security Law

Passed on June 10, 2021, in effect since September 1, 2021

What's New: New data classification categories aimed at protecting national security are loosely defined, leaving interpretation up to Chinese authorities.

The DSL references two main categories of sensitive data—national core data and important data—with new guidelines for governing each.

- "National core data" is defined as data concerning national security, economic interests, Chinese citizens' welfare, or the public interest, and is categorized as the most sensitive data type.
- "Important data" is categorized as the second most sensitive data type but is not clearly defined in the

text. Instead, regulatory authorities at the local level are expected to issue additional guidelines as to what constitutes important data for their jurisdiction, but the timeline for issuing the guidelines has not yet been determined.

The new data categorization system poses two primary issues for companies operating in China. The first is the lack of definitional clarity. There are fines of up to RMB 10 million (~$1.56 million) per infraction for mishandling national core data, but compliance will be difficult given the vague definition. The same holds true for important data, where violations can include fines of up to RMB 5 million (~$780,000), but definitions are even less clearly defined. Until concrete examples of the law being applied are available, or clarifying definitions are issued, businesses will be left with unclear information to make strategic adjustments in the interim. Second, allowing local regulatory bodies to determine what constitutes important data creates another layer of compliance requirements. It will also make operating across jurisdictions more complex if different definitions are adopted. Both international and domestic companies will now be forced to navigate existing national guidelines, alongside a yet-to-be-determined number of region- and industry-specific guidelines.

Old idea, new reach: The Data Security Law builds on the provisions of the Cybersecurity Law and expands China's extraterritorial reach over new categories of data.

The DSL expands on previous data localization and data transfer rules and imposes harsher penalties for violations. Companies that handle these types of data (for example, those operating in fields related to physical or digital infrastructure or natural resource extraction) are responsible for ensuring that all data generated within China is stored within the country. A security assessment in accordance with the Cyberspace Administration of China's guidelines is required before any China-originated data is transferred abroad.

Critically, all data handlers are prohibited from providing any data stored in China to foreign government agencies without approval from Chinese government authorities, regardless of the data's sensitivity level and where the data was originally collected. This guideline is widely viewed as a direct counter-measure to the U.S.'s 2018 Clarifying Lawful Overseas Use of Data Act (the "CLOUD Act"). Under the CLOUD Act, U.S. law enforcement agencies are given the legal right to demand access to electronic data, no matter which country the data is stored in. China's new legal requirements create the potential for international companies to be caught between conflicting demands from U.S. and Chinese authorities when it comes to access to sensitive data.

How it's enforced: Fines and legal penalties for breaching the laws are significant, but initially enforceability is likely to be inconsistent.

Companies that provide national core data to foreign officials without approval from Chinese authorities are subject to fines as well as the potential forced shutdown of their businesses and potential criminal charges. For violations regarding important data, additional penalties may be added directly to the individuals involved as determined on a case-by-case basis by Chinese authorities. There are also penalties for companies that fail to cooperate with data requests from Chinese authorities on law enforcement or national security matters, but the extent of these penalties is not clearly defined. Instead, parties found to be in violation will be prosecuted in Chinese courts.

The Personal Information Protection Law

Passed on August 20, 2021, in effect since November 1, 2021

What it's based on: Modeled after the EU's General Data Protection Law (GDPR), the Personal Information Protection Law is China's first comprehensive data protection law covering personal data.

The PIPL covers all data activities related to the personal information of Chinese citizens, whether it is originally collected within China or abroad. The law governs data collection from both public and private companies and includes provisions mandating that Chinese government agencies notify and obtain consent from individuals. However, the provisions related to Chinese government data collection do not apply in situations where it is necessary for "acting in the public interest." In practice, this means that the law is unlikely to end the Chinese government's extensive data collection practices ranging from collecting biometric data from facial recognition software to the myriad data points that make up citizens' social credit scores.

Similar to the GDPR, the PIPL includes provisions granting the right to limit or refuse processing of personal information, the right to refuse automated decisions regarding personal data, and the requirement to obtain explicit consent before transferring personal data to third parties. It also includes more severe penalties for violation than the GDPR. Companies found in violation of the law face fines up to RMB 50 million (~$7.8 million) or 5 percent of revenue and risk suspension of their operations. Additionally, the legal ramifications may be reflected in companies social credit scores, which impacts their ability to access financing. Individuals can also be held liable for violations, with monetary fines up to RMB 1 million (~$157,000) as well as additional discipline determined by legal authorities.

Why it's concerning: New deletion requirements on personal data and transparency rules could disrupt

business models that rely on collecting and selling consumer data.

Under the PIPL, data handlers are now required to delete personal data after the stated purpose for collection has been completed. How this will be determined is left ambiguous, making it unclear whether this represents a legitimate data privacy benefit for individuals. Depending on when data needs to be deleted, and the stringency with which this provision is enforced, it could disrupt data economy companies that rely on storing, analyzing, and selling user data. Additional restrictions for safeguarding individuals' data are determined based on the company's categorization—whether it is a "major internet service platform," has a "large number" of users, or engages in "complex business activities." With these categories not clearly defined in the text, like many parts of the PIPL and DSL, they are likely to be interpreted at the discretion of Chinese authorities.

What this means: Transferring personal data outside of China is more difficult under the PIPL, and its adoption encourages other countries to enact similar personal data protection measures.

Transferring personal data within China or overseas now requires the data subjects' informed consent. This is similar to a provision in the GDPR, which forced many businesses to add consent forms and update their data collection policies. For overseas transfer, companies are responsible for ensuring that the country that data is being sent to has data protection requirements at least as stringent as the PIPL. This requirement has been included in a variety of personal data protection laws globally, including in the GDPR, and EU authorities have enforced significant fines on companies that violate this provision. As more countries adopt similar provisions in their data protection laws, the pressure to pass comprehensive data protection laws globally mounts. The PIPL includes an additional restriction on companies that are deemed to be in possession of a "large volume" of personal data. For those companies, a mandatory security review by the Cyberspace Administration of China must be completed before transferring any data overseas.

The Big Picture and Implications for Businesses

The addition of new data classifications, legal jurisdictions, and data storage requirements imposes another layer of regulatory complexity for businesses operating in China.

China's new data security laws increase the complexity of the data governance regulatory landscape. The size and significance of China's economy, as well as the addition of both national- and regional-level guidelines, will potentially require major adjustments for data economy companies doing business in China.

China now joins the EU as a major economy with a comprehensive data governance framework, with India likely to be the next major economy to follow suit—its comprehensive Data Protection Bill is expected to be passed in the first half of 2022. As more countries pass data protection laws, effectively navigating the web of regulations will become a prerequisite for operating in the global digital economy.

For a full breakdown of the global data governance regulatory landscape, see FPA's Global Data Governance Policy Database. And for a comprehensive breakdown of the key factors determining the future of international data governance, see FPA's Global Data Governance Power Map. ■