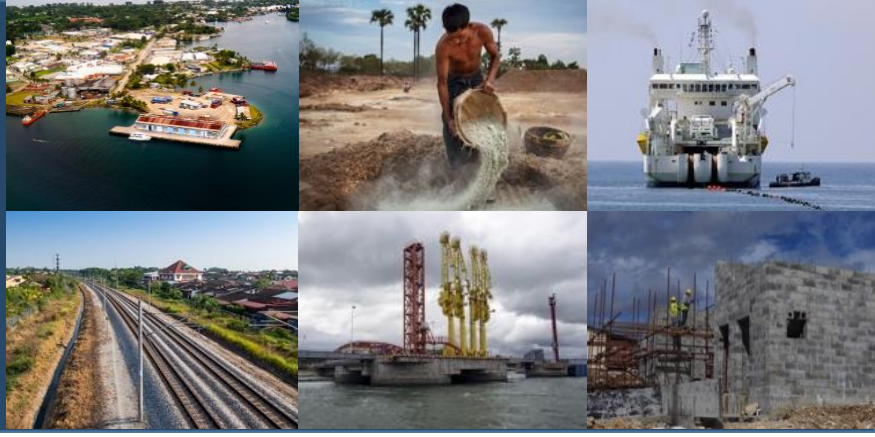
BRI MONITOR

POLICY BRIEF:
CHINA'S DIGITAL SILK ROAD



BRI Monitor is a joint initiative started by think tanks in Asia and the Pacific to track the impact of China's Belt and Road Initiative projects. A key aim is to promote transparency and accountability around the terms and full costs to countries and communities. With support from the Center for International Private Enterprise, BRI Monitor partners developed a new methodology to assess the level of disclosure about various infrastructure projects and contract data. This can help identify governance gaps that make countries vulnerable to corrosive capital situations.

HEIGHTENED RISKS AND MITIGATION TOOLS

In his keynote speech at the 2023 Belt and Road Forum for International Cooperation, Xi Jinping formalized a change in direction for the Belt and Road Initiative (BRI), the Chinese leader's signature foreign policy initiative. Priorities are moving away from infrastructure mega-projects and toward investments that are smaller, more economically viable, and that position China as a leader in the emergence of a global digital economy. Some state-owned firms and companies with strong ties to the Chinese Communist Party are already making substantial investments in 5G network infrastructure, e-commerce, and the digital economy worldwide.

China's digital service offerings, which are often referred to as the Digital Silk Road, hold significant appeal for nations seeking solutions in areas like cloud computing, data center management, data analysis for smart city initiatives, and establishing harmonized regulatory frameworks for digital cross-border trade. These offerings are a cheaper alternative to U.S. and European options for rapid digitalization. However, cybersecurity vulnerabilities and privacy violations raise concerns about the risks of using equipment manufactured in China.

Consequently, a small but growing list of countries, including all Group of Seven states and more than a third of European Union members, have banned the use of telecommunications equipment from Chinese providers Huawei and ZTE as of June 2023. EU officials call for others to follow suit. In Southeast Asia, the Philippines is a frequent target of cyberattacks, and BRI Monitor case studies by CIPE partner Stratbase ADR Institute illustrate the risks at both the national and individual levels. In one controversy, DITO Telecom, a telecommunications consortium with 40 percent ownership by a Chinese state-owned enterprise (SOE), installed Chinese equipment atop mobile-phone towers inside and adjacent to Philippine military bases. Critics of another initiative, the now-scrapped "Safe Philippines" project, raised concerns around the security and privacy of Filipinos' data that would be captured using Huawei technology.

Countries should be able to enjoy the convenience and opportunity technology provides —including Chinese versions—without fearing for their national security or their citizens' personal privacy. Unfortunately, China's reputation means that governments that use Chinese technology must take extra steps to protect themselves, their citizens, and their data. While there is no easy solution, well designed and implemented laws, procurement rules, and investment screening procedures can be a good place to start.

THREATS TO CYBERSECURITY: THE CASE OF DITO TELECOM

When former Philippine President Rodrigo Duterte took office in 2016, he vowed to break up the country's telecommunications duopoly by allowing a third operator to enter the market. After a flawed bidding process in which nine other contenders either dropped out or were disqualified on technicalities such as missing application documents, the Mislatel Consortium—now known as DITO Telecom—emerged as the winner. DITO is controlled by two Philippines-based companies owned by Dennis Uy, a major financial supporter of Duterte; and by the PRC state-owned enterprise China Telecommunications Corporation (China Telecom), which holds a 40 percent stake.

China Telecom's membership in the conglomerate raises questions about China's ability to threaten Philippine cybersecurity and undermine the country's democracy. For example, the Armed Forces of the Philippines (AFP) has allowed DITO to join the Philippines' other providers in installing network infrastructure inside military bases despite concluding in its own risk analysis that vulnerabilities in AFP systems could be exploited. Under Article 7 of China's 2017 National Intelligence Law, all Chinese citizens and companies are required to "support, assist and

cooperate with state intelligence work" without regard for geographic boundaries. Consequently, the PRC government could mandate that China Telecom hand over data gathered through DITO installations. The possibility that China could gain access to sensitive military information—it may have already—is particularly striking in the Philippines, where maritime and territorial disputes lead to regular confrontations between the two countries. Even so, DITO Telecom currently has multiple cell towers operating with Chinese equipment inside AFP bases.

Even outside of military installations, the security risks to the Philippines and other countries that source their digital infrastructure from China will continue to grow as the state's cyber capabilities expand and its government grows bolder in the use of digital tools to undermine democracy. Cybersecurity firm CrowdStrike has documented a surge in China-linked cyber-attacks in recent years, and in 2022 China was by far the dominant origin of cyberattacks. China-linked cyber criminals targeted nearly every global industry sector and geographic region that CrowdStrike tracks. The proliferation of Chinese technology abroad will only make it easier for these groups to conduct malicious activity. While Chinese telecoms firms promise to provide digital connectivity at low prices, states clearly foot the bill through costs to their national security and cybersecurity.

THREATS TO PERSONAL SECURITY AND DATA PRIVACY: SAFE PHILIPPINES

During the Duterte administration, the Philippine Department of Interior and Local Government (DILG) entered into a now cancelled USD$396.8 million agreement with China International Telecommunication Construction Corporation (CITCC) to fund the installation of a network of security cameras, in what has been dubbed the "Safe Philippines" project. Since its inception, the project had sparked concerns about personal security for Filipino citizens because the provider of the security cameras, Huawei, has faced scrutiny in the United States, Japan, Australia, and a number of countries across Europe due to allegations of hacking and spying.

Filipino citizens and a skeptical senator voiced concerns that data collected through Safe Philippines infrastructure might be used for Chinese intelligence purposes. Among the concerns expressed were that the project's bidding process may have violated the 2016 Revised Implementing Rules and Regulations (IRR) of Republic Act No. 9184 by restricting eligible bidders to Chinese entities, an indication of the program implementers' willingness to heed Philippine law, including ones protecting personal security and privacy, such as the Data Privacy Act. The prospect of surveillance equipment manufactured by Chinese companies further exacerbated concerns that personal information could be collected and misused by actors in both China and the Philippines. While Safe Philippines attempted to prevent traditional crime through increased surveillance, it may have also increased the threat of cybercrime in one of the world's most targeted countries.

BALANCING THE RISKS AND OPPORTUNITIES OF INVESTING IN DIGITAL INFRASTRUCTURE

For most countries, building an entirely domestic telecom industry that is robust and competitive is an exceedingly difficult challenge. Providing adequate services will require countries to rely in part on foreign investment, and BRI loans will continue to be an attractive option as China pivots its focus toward global digital infrastructure. It will therefore be critical for host countries to understand their vulnerabilities and prevent unintended consequences.

The Philippines' recent move to develop its second five-year cybersecurity strategy—complete with a public comment period—is a step in the right direction. The draft plan is built around six pillars, including one focused on raising public awareness of cyber threats and best practices. Informed and engaged citizens are critical to maintaining national cybersecurity, both by bringing their knowledge and skills to the workplace—thereby reducing the burden of training them there—and by enhancing public scrutiny of organizations' cybersecurity practices. As the public backlash that helped to end the Safe Philippines project demonstrates, broad awareness is pivotal to ensuring that security risks are addressed swiftly and decisively.

The plan also calls for identifying and securing the Philippines' critical infrastructure. This is not a one-time process. Technology progresses rapidly, with existing vulnerabilities discovered and new ones emerging daily. Countries must therefore devote adequate resources to regular risk assessments. The results should be made publicly available to keep governments accountable.

Collaborating with civil society and the business sector to establish inbound investment screening processes offers states a way to protect themselves from corrosive capital. An effective screening regime should incorporate the views of civil society and domestic business leaders, to help ensure continuity across government administrations. Philippine civil society organizations have had success before, such as their advocacy for safeguards on foreign ownership of public utilities ahead of a 2022 amendment to the Philippines' Public Service Act.

Finally, the bidding process for DITO telecom reveals how cumbersome rules and regulations can stifle competition and lead to outcomes in which powerful foreign operators—and untrustworthy Chinese vendors in particular—become a country's only option. By the Philippine government's own account, DITO Telecom was the only bidder that met all requirements to become the country's third telecom provider. Governments have a responsibility to ensure national security and cybersecurity for their citizens—but they must also create ecosystems in which new entrants with innovative ideas can challenge the dominance of established players. States in a similar position to the Philippines should therefore consider reforming their procurement rules to enable greater competition and open space for firms to bring fresh, constructive capital to the table.

*BRI Monitor founding members include the Institute for Democracy and Economic Affairs (IDEAS) in Malaysia, Future Forum in Cambodia, Institute of National Affairs (INA) in Papua New Guinea, Sandhi Governance Institute in Myanmar, and Stratbase ADR Institute for Strategic and International Studies (ADRi) in the Philippines. To view their latest research and sign up for newsletters and briefs, visit **brimonitor.org** or email **contact@brimonitor.org**.*