



Nuclear power and telecommunications **SECURITY CONCERNS ABOUT CHINESE INVESTMENTS**

China actively seeks to expand its overseas investment in critical infrastructure. This involvement makes host countries uneasy especially in the West, even though financial benefits sometimes override broader national interests and security issues.

China's attempts to invest in overseas critical infrastructure, defined as infrastructure closely related to sovereignty and national security, has become a sensitive issue to host country governments particularly in the West. They fear that Chinese investment in nuclear and telecommunications infrastructures entails consequences for nuclear security and safety and information security respectively. This policy brief provides an overview of how various countries have

RECOMMENDATIONS

- Host country governments should conduct their own assessments of security implications of Chinese involvement in critical infrastructure.
- The host country government should work with Chinese companies to set up high security and safety standards in collaboration with regional or international organisations.
- Security measures should be regularly monitored and not bypassed for contingencies or commercial processes.
- Increase the transparency of commercial deals with Chinese companies in order to avoid public outcries and criticism.

More caution towards Chinese nuclear investment is expected from Western countries, as nationalism and protectionism are on the rise

Thus far, scrutiny of Huawei and ZTE in the US, UK and other countries have not published non-classified information that is solid evidence of Chinese espionage through its telecom companies' involvement in telecom infrastructure.

received Chinese interests in nuclear power and telecommunication industries.

NUCLEAR POWER

China is building a large number of nuclear plants within its borders and actively seeking to construct or export nuclear power stations overseas. The domestic boom is part of an effort to diversify energy usage and reduce pollution, while overseas investment is aimed at exporting nuclear capacity, technology and construction services, as well as strengthening political and economic ties with certain countries. Chinese nuclear companies are big state-owned enterprises, supported by the state with financing from policy banks or state commercial banks as well as the state's active diplomacy.

Used as a foreign policy tool, Chinese overseas nuclear investment enables China to obtain oil and gas resources and to enhance relations with a range of host countries in Asia, the Middle East, Central Asia, Africa and Europe. In particular, China prioritises countries along the new Silk Road. Chinese nuclear investment is attractive to developing countries because of its large capital and competitive price. In terms of nuclear safety, China prides itself on having built and run many reactors domestically without major accidents, but its overseas record is limited. China's involvement in overseas nuclear projects has mainly been to contribute capital and construction workforce, to fit with Western designs. However, it has now started to export its own technology, with two plants under construction in Pakistan and more contracted with other countries. Because China is using its latest technology when building nuclear plants both overseas and domestically, it is

too early to judge its safety. Moreover, this rapid development is taking place despite a recent Chinese official document pointing out inadequate disaster response programmes within China.

As for nuclear proliferation, China is a member of the Nuclear Nonproliferation Treaty and the Nuclear Suppliers Group (NSG). It was suspected of providing nuclear technology to Iran, North Korea and Pakistan in the early years of the communist regime, but the current government does not wish neither Iran nor North Korea to possess nuclear weapons. Beijing encourages a peaceful nuclear programme in Iran after the latter reached a nuclear agreement with major powers in January 2016. China's export of nuclear technology to Pakistan, however, raises international concerns because Pakistan has been a source of proliferation despite the government's denial of involvement. Even though the NSG allowed China to build the first two plants in Pakistan as an exception to its rules, China is now going beyond this exemption and the risk of proliferation depends on how Pakistan and other countries like Iran use their newly obtained technology.

China is an important market for nuclear companies from the West. Although the US has indicted a Chinese for illegally obtaining nuclear technology and warned against technology leakage, Western companies will continue to try to get a share of China's domestic nuclear boom. In the UK, the Hinkley Point nuclear plant will go ahead after a change in government and another round of security reviews. Higher levels of caution towards Chinese nuclear investment is expected from other Western countries as well, as nationalism and protectionism are on the rise, and as

the governments are uncertain about the security or strategic implications of letting Chinese nuclear companies into this critical sector.

The same could be said about uranium and rare earth exports to China, the area where China has a major interest in Greenland. The Greenlandic government has been interested in inviting Chinese investment in mining rare earth that contains uranium for several years, and the Australian company operating in Greenland has signed MOUs with two Chinese state-owned enterprises on uranium production. The new agreement between Greenland and Denmark reached in 2016 puts more checks on the export of uranium and rare earth to China. How much China can tap into the rare earth minerals in Greenland depends therefore on the interpretation and application of the new rules. This has both economic and diplomatic implications for Greenland, Denmark and China.

TELECOMMUNICATION

Across Western countries, Chinese interest in telecom infrastructure has been received with skepticism because of information security concerns. While ZTE is a state-owned company allegedly operating on purely commercial terms, it is more difficult to determine the degree of influence of the Chinese state on Huawei. Thus far, scrutiny of Huawei and ZTE in the US, UK and other countries have not published non-classified information that is solid evidence of Chinese espionage through its telecom companies' involvement in telecom infrastructure. There are concerns, however, about Chinese government having indirect influence on the companies, and about loopholes in Chinese technology, which could be abused by hackers. Ironically, in the process of investigating Huawei, the US hacked into the Huawei system for seven years and considered using it for future espionage or cyber-attack activities in countries that use Huawei equipment.



Namibian information minister Tjekero Tweya cuts the ribbon for Huawei Demo Truck during the official opening of the 2016 ICT summit, in Windhoek, Namibia, on Oct. 10, 2016. China's tech giant Huawei signed a memorandum of understanding with Namibia information ministry for driving information and communication technology development and promoting technological literacy in the country. (Xinhua/Wu Changwei)

Chinese involvement in overseas telecommunication differs greatly on the depth and scope from country to country. In the US, both ZTE and Huawei are banned from bidding on government contracts, and the government advises private companies against using them due to potential security risks. In the UK, the commercial engagement of Huawei is significant; the company's Cyber Security Evaluation Centre (the Cell) has been established here, and security experts cleared by the UK government check all Huawei equipment for security. The Cell is also used to service other countries such as Scandinavia, where Huawei's involvement continues to grow. In Africa, Chinese engagement has widely been welcomed, not least because of the cheap provision of infrastructure and smartphones. There is, however, a risk that Chinese telecom companies provide authoritarian governments with systems that can be used for surveillance and oppression, as we have seen in Ethiopia.

In Denmark, the rules governing TDC's cooperation with Huawei is, at least on the surface, quite significant, with security measures likely beyond those that Huawei work under in the UK. These include screening of hardware in The Cell in the UK, full authority of the Center for Cyber Security to monitor Huawei and network activities, and the return of network control

from Romania (where it had been outsourced to) back to Denmark in a Network Operation Center (NOC), where security-cleared Huawei employees work alongside Danish employees from TDC. These measures are important to ensure continued monitoring and control over a critical part of Danish infrastructure. The current mechanism also requires the company's voluntary compliance, which was put into question in 2015 when the Danish Broadcasting Corporation (DR) found several instances of non-security-cleared individuals working within the NOC. The dilemma, especially in Denmark and elsewhere in Europe, remains that no other companies can provide advanced technology at the competitive prices that Huawei and ZTE can. Denmark and other Western countries still need to balance security considerations with the trade and economic interests of the country.

Yang Jiang, senior researcher, DIIS

Aki Tonami, associate professor, Tsukuba University

Adam Moe Fejerskov, researcher, DIIS

Coverphoto: Workers walk by the No.3 and No.4 power generation units of the Hongyanhe Nuclear Power Station in Wafangdian of Dalian City, northeast China's Liaoning Province, Sept. 22, 2016. The first phase of the Hongyanhe Nuclear Power Station project, the first nuclear power plant in northeast China, is completed. (Xinhua/Pan Yulong)

