

This report is written by Yang Jiang, Aki Tonami, Adam Moe Fejerskov and published by DIIS as part of the Defence and Security Studies.

Yang Jiang is Senior Researcher at DIIS Aki Tonami is Associate Professor, Tsukuba University Adam Moe Fejerskov is PhD, Researcher, DIIS

DIIS · Danish Institute for International Studies Østbanegade 117, DK-2100 Copenhagen, Denmark Tel. +45 32 69 87 87 www.diis.dk

Layout: Lone Ravnkilde & Viki Rachlitz Printed in Denmark by Eurographic Danmark

ISBN 978-87-7605-847-0 (print) ISBN 978-87-7605-846-3 (pdf)

DIIS publications are available for free on diis.dk

© Copenhagen 2016, the authors and DIIS

## **Table of Contents**

Introduction	5
China's interests and activities in nuclear power	7
Globalisation of Chinese telecom companies	10
China's investment in overseas nuclear power	13
Uranium projects in Greenland	14
Hinkley Point in the UK	17
Non-Western countries: Pakistan, Saudi Arabia, Iran and Ukraine	20
Discussions on nuclear power	24
Chinese investment in overseas	29
telecommunications infrastructure	
Scandinavia	30
Huawei in Denmark	30
Huawei in Sweden and Norway	33
Not so successful attempts to enter the US	34
China's investment in telecommunications: UK	36
Chinese involvement in African telecommunications infrastructure	38
Chinese involvement in Ethiopian telecommunications	40
Discussions on telecommunications	41
Conclusion	45
Notes	50



As China expands overseas investments, their involvement in other countries' critical infrastructure such as telecommunications and nuclear power increases. In many host countries, this has become a sensitive issue for governments and media, in particular in Western countries. In their view, Chinese investment in nuclear and telecommunications infrastructures entails consequences for nuclear security and safety and information security respectively. Here, nuclear security refers to the prevention and response to theft, sabotage, unauthorised access and illegal transfer of nuclear material and facilities. Nuclear safety refers to proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation hazards. Information security refers to the prevention of and response to unauthorised access by state and non-state entities to critical information and critical government infrastructures. Accordingly, many countries have procedures for reviewing intentions of foreign investment in their critical infrastructure, defined as infrastructure that is closely related to issues of sovereignty and national security.

As will be covered in this report, host country attitudes towards Chinese investment in telecommunications and nuclear power vary widely. Some countries reject Chinese investment in these areas because of distrust in Chinese companies based on their perceived connection to the Chinese government, and others have accepted them due to economic needs and diplomatic relations with China. In particular, Chinese companies are aggressively seeking entrance into the European market because they have gathered experience in developing countries and perceive individual European countries as the doorstep towards the developed world at large, given the latter's economic slowdown. European countries may find Chinese companies to be the only serious bidders for expensive, low-profit and long-term infrastructure projects. Denmark, for one, has gone through debates on Chinese investment in its telecom infrastructure, and seeing that bilateral ties to Chinese companies will only continue to deepen, questions around implications for security will continue to remain pertinent for decision-makers.

This policy report therefore provides an overview of how various countries have received Chinese interests in investing in their critical infrastructure, using the examples of the nuclear power and telecommunication industries. For nuclear power and uranium mining, the report reviews the latest Chinese investments (planned or realised) in the UK, Greenland, Pakistan, the Middle East and Ukraine. For telecommunications, the report analyses the wide range of responses from countries - the Scandinavian countries, US, UK, and selected African countries - to Chinese

companies' interests in building telecom infrastructure there. Based on these empirical cases, the report discusses the implications for national and international security, and comes up with policy recommendations for Denmark.

Before we dig into the specific cases, an overview of China's activities and apparent interests in nuclear power and telecom globalisation is provided in the next two subsections.

#### CHINA'S INTERESTS AND ACTIVITIES IN NUCLEAR POWER

China's economic growth, albeit slowing, continues to demand a huge amount of energy supply. Nuclear power is identified by the government as a strategic energy source for reducing pollution and reliance on fossil fuel imports. Since the 1990s, China has relied on foreign design and technology to build nuclear power stations within China. As of August 2016, there are 35 nuclear reactors in operation and another 22 reactors under construction. China has served as a big market for international nuclear companies including US-based, now Japanese-owned, Westinghouse Electric and France's Areva. Although in April 2016 the US government charged CGN with conspiracy to obtain illegal nuclear reactor building plans to help design their own reactor Hualong One, China is the biggest growth market for nuclear power and international giants are still expected to compete for contracts with China even at the risk of sharing technology.<sup>2</sup>

The experience of building many reactors within the country, combined with lower costs of labor and capital, makes Chinese nuclear reactors potentially attractive to international customers.

Based on foreign technology and their own original research, China has developed its own third generation reactors, including reactors Hualong-1, CAP1400, and a high-temperature gas-cooled reactor design. For instance, Westinghouse has signed a technology transfer agreement and later entered into a joint venture with the State Nuclear Power Technology Corp (SNPTC) to build the AP1000 and its Chinese spin-off called the CAP1400. After the Fukushima Daiichi nuclear disaster in Japan in 2011, China froze all new plant approvals. However, soon new plants are planned, with a target of 110 plants by 2030, overtaking the US, which has 100. In

July 2015, China announced its new targets for renewable energy and nuclear power for further cutting down carbon emission.<sup>3</sup> Its Five-Year Plan also revealed the government's goal to increase China's nuclear power capacity from 28.3 gigawatt in 2015 to 58 gigawatt by the end of 2020.<sup>4</sup>

The ambitious plan of nuclear plant construction means China needs a large amount of uranium supply, some of which needs to come from overseas. In 2010, China needed 3600 tons of uranium (tU). In 2020, the demand is expected to be 15,000 tU. According to the Bureau of Resources & Energy Economics in Australia (a major exporter of uranium to China), the growing use of nuclear fuel for power generation in China will push up global uranium demand by 42% by 2017.

All this rapid development is taking place despite insufficient safety controls. In its first white paper on nuclear emergency response, published in January 2016, China said the existing disaster response capability (in terms of technology, equipment, human resource, and standards etc.) was "inadequate" to cope with "a new situation and challenges". The government also delayed the construction of two reactors in Taishan, Guangdong province, due to safety concerns and public protests.<sup>5</sup>

The experience of building many reactors within the country, combined with lower costs of labor and capital, makes Chinese nuclear reactors potentially attractive to international customers, particularly in an international environment where building nuclear plants has become extremely expensive and requires large-scale financial assistance from the state.<sup>6</sup> China can offer such assistance while existing major nuclear power exporters, namely US, France and Japan, have become weaker in comparison, according to Gregory Jaczko, a former Chairman of the US Nuclear Regulatory Commission.<sup>7</sup>

Through the National Development and Reform Commission (NDRC), a ministerial level policymaking agency, China implements a determined policy of exporting nuclear technology with Chinese intellectual property rights, supported by diplomatic efforts and state financial resources.<sup>8</sup> As Chinese technology does not yet enjoy a reputation comparable to established players such as Canada, France, Russia, South Korea, and the US, the pattern of Chinese participation in overseas nuclear projects has consisted in the use of foreign-designed reactors but Chinese money and construction expertise.<sup>9</sup>

## **Export sales and prospects for Chinese nuclear power plants**

COUNTRY	PLANT	TYPE	EST. COST	COMPANY	STATUS FINANCING
Pakistan	Chasma 3&4	CNP-300	\$2.37 billion	CNNC	Under construction, Chinese finance 82% of \$1.9 billion, Exim-Bank
	Karachi Coastal 1&2	Hualong One	\$9.6 billion	CNNC	First unit under construction, \$6.5 billion vendor finance, maybe 82% China finance, Exim-Bank
Romania	Cernavoda 3&4	Candu 6	€7.7 billion	CGN	Planned, to complete part-built units, Chinese finance, Exim-Bank and ICBC, Nov 2015
Argentina	Atucha 3	Candu 6	\$5.8 billion	CNNC	Planned, with local involvement and \$2 billion Chinese financing, ICBC
	Atucha 4 or other site	Hualong One	\$7 billion	CNNC	Vendor financing envisaged, ICBC in lead role
UK	Bradwell	Hualong One		CGN	Promised future opportunity
Iran	Makran coast	2 x 100 MWe		CNNC	Agreement July 2015
Turkey	Igneada	AP1000 and CAP1400		SNPTC	Exclusive negotiations involving Westinghouse, 2014 agreement
South Africa	Thyspunt	CAP1400		SNPTC	Prepare for sumitting bid
Kenya		Hualong 1		CGN	MOU July 2015
Egypt		Hualong 1		CNNC	MOU May 2015
Sudan		ACP600?		CNNC	Framework agreement May 2015
Armenia	Metsamor	1 reactor		CNNC	Discussion underway
(No country)		HTR600		CNEC	Export intention
Kazakhstan		Fuel plant JV		CGN	Agreement Dec 2015

Source: World Nuclear Association, 'Nuclear Power in China', updated 29 July 2016, http://www.world-nuclear.org/information-library/country-profiles/countries-a-f/china-nuclear-power.aspx

Unsurprisingly, Chinese nuclear companies are state-owned, including the three largest ones: China National Nuclear Corporation (CNNC), China General Nuclear (CGN), and State Power Investment Cooperation (SPIC). According to the president of CNNC, China aims to build 30 nuclear power units in countries involved with its Silk Road Initiative by 2030, and it will actively promote localisation of the technology and strive to establish an integrated industrial system for these countries. <sup>10</sup> Their bid for nuclear plants in Western countries naturally stirs up debates, a notable example being the Hinkley project in the UK, as will be discussed in detail later.

CNNC has reached bilateral agreements on nuclear energy cooperation with countries including Argentina, Brazil, Egypt, Romania, France and Jordan. CGN and CNNC have entered into agreements with Romania and Argentina to build Canadian designed CANDU-6 reactors. Some of these projects were initiated by non-Chinese companies but stalled due to financial difficulties. China's offer of financing (e.g. through generous concessional loans provided by China's Development Bank, Exim Bank and state commercial banks) and construction services, and occasionally technology, has revived some stalled projects.

China hopes to gain experience and reputation through these foreign-designed projects in order to eventually sell its own designed reactors. In fact, China is exporting its nuclear technology to developing countries to demonstrate their safety. Argentina has agreed to build a Hualong-1 at the Atucha site in Buenos Aires province. As will be discussed later, China has made most progress in Pakistan, where two Chinese small-sized reactors built by CNNC are already in operation and two more are under construction.

#### **GLOBALISATION OF CHINESE TELECOM COMPANIES**

In the early years of China's 'going out' push for overseas investment, telecommunications and transportation infrastructure projects were often used as part of an aid-and-investment package, in exchange for the host country's energy and natural resources. Huawei and ZTE are the two biggest telecommunications and network equipment and services providers based in China. Huawei is privately owned, or officially 'employee owned' though the ownership structure is exceedingly complex. ZTE is state-owned, though as a publicly listed company it has aimed to function as a profit-driven enterprise.

Huawei is now the world's largest telecommunications company after overtaking Ericsson in 2012. The company has offices in 140 countries in the world and has 140,000 employees. Huawei is much bigger than ZTE: its 2015 revenue was over \$60 billion, with 60% coming from outside of China. Huawei now accounts for more than 50% of Europe's 4G mobile communications system. ZTE's 2015 revenue was about \$15 billion, with half of it from overseas. In view of their progress of globalisation, the government intensified its diplomatic and financial support for Huawei and ZTE to become 'global champions'. 'Connectivity' is one of the central concepts of China's latest One Belt One Road initiative.

Concerns related to Huawei have to do with its perceived links to the Chinese government and military. This is mainly due to the fact that Huawei was founded in 1988 by Ren Zhengfei, a former deputy director of China's People's Liberation Army engineering corp. <sup>11</sup> Today, China is suspected by Western countries to be one of the main perpetrators of state-sponsored cyber-attacks, focusing on espionage and information acquisition. In this regard, the perceived links between Huawei and the Chinese government are worrying to Western countries and create doubts about Huawei's intentions, whether commercial or political. <sup>12</sup>

The perceived links between Huawei and the Chinese government are worrying to Western countries and create doubts about Huawei's intentions, whether commercial or political.

Both companies have grown quickly with government financial and political support within and outside China. They both started global expansion in developing countries first, but have in recent years strengthened efforts to get into developed country markets, where they have been met with more resistance because of protectionism or national security concerns. As will be discussed later, the US has virtually banned them from being part of its telecoms infrastructure since 2012. Other Western countries, including US allies, vary a lot in their attitude, with Australia being very cautious and UK the most welcoming.



### **URANIUM PROJECTS IN GREENLAND**

Greenland's economy currently relies on seafood exports and the block grant from Denmark. Achievement of economic growth is critical for Greenland because it wants to achieve a more 'self-sufficient economy' in order to achieve more political independence from Denmark. <sup>13</sup> Moreover, due to demographic changes, its economy is predicted to be in huge deficit by 2040. In order to maintain the current level of public services, Greenland will need additional DKK 800 million per year (on average) over the next 25 years. <sup>14</sup>

In recent years, Greenland has been actively seeking to transform itself from a fishing society to a mining economy. Global warming and ice melting in areas of Greenland have made this transformation possible. Although it is difficult to evaluate the economic potential of Greenland's natural resources due to fluctuation of global commodity prices, experts assure that "[i]f all goes well, the extraction of hard minerals could begin to contribute significantly to Greenland's economy within five to ten years."<sup>15</sup>

Despite many controversies surrounding uranium mining as well as the idea of using foreign capital in its pursuit, Greenland gradually paved the way for its realisation.

Greenland enjoys Self-Rule based on the Greenland Self-Rule Act enacted in 2009, which grants the rights for Greenland to manage all natural resources in Greenland as well as the economic zone off its coast. However, uranium mining by foreign companies and uranium export have been controversial as it has potential security and foreign policy implications beyond Greenland and to the Kingdom of Denmark, which is bound by the Non Proliferation Treaty (NPT) administered by the International Atomic Energy Agency (IAEA). In the case of uranium export, IAEA requires that a uranium exporting country needs to conclude international nuclear agreements with a recipient country. There was a difference in opinion between Copenhagen and Nuuk, the capital of Greenland, with regards to who should be responsible for the negotiation and conclusion of such agreements. According to Copenhagen, Denmark should be in charge, as the Greenland Self-Rule Act sections 12(4) and 13 stipulate that agreements affecting defence and security policy are to be negotiated and concluded by the Danish government (with the involvement of Nuuk), while Nuuk's position was that such agreements concern only Greenland.<sup>16</sup>

Despite many controversies surrounding uranium mining as well as the idea of using foreign capital in its pursuit, Greenland gradually paved the way for its realisation. During the administration of Premier Kuupik Kleist (12 June 2009 - 5 April 2013), Greenland maintained the Danish practice and abstained from mining uranium. However, it passed a law known as the Large Scale Projects Act to facilitate the immigration and management of large numbers of foreign workers needed to build and operate the mines, in view of a future possibility of opening mining sites with non-Greenlandic workers. <sup>17</sup> After the elections in 2013, during which the issue of mining became an important point of discussion, Alega Hammond became the new Premier. During her administration (5 April 2013 - 30 September 2014), the policy direction was to further accelerate Greenland's transformation to a mining economy, particularly by attracting foreign investment. As a result, on October 24, 2013, Greenland's legislature overturned a 1988 ban on the mining of radioactive materials, which meant minerals including uranium, thorium, and rare earth deposits could now be mined in Greenland. 18 Among potential foreign investors, Nuuk regarded China as one of the most prospective candidates. In November 2013, Jens-Erik Kirkegaard, Minister of Industry and Minerals of Greenland, made an official visit to China to attract Chinese investment to its mining industry. According to Kirkegaard, "the island has large amounts of mineral resources while China's economic development needs such resources to maintain growth."

Against this background, on 24 March 2014, Greenland Minerals and Energy Limited (GMEL) and China Nonferrous Metal Industry's Foreign Engineering and Construction Co. Ltd. (NFC, a state-owned enterprise that specialises in overseas engineering contracts and mining projects) signed a non-binding Memorandum of Understanding (MoU) to cooperate in aligning the rare earth component of GMEL's Kvanefjeld Project with NFC's rare earth separation experience and capacity. GMEL is an Australian domiciled mining company that has been operating in Greenland since 2007. It has approximately 50 employees and mainly focuses on the Kvanefjeld multi-element project (rare earth elements, uranium, zinc). Kvanefjeld is located in Southern Greenland and it is by far the most advanced uranium project in Greenland. GMEL asserts that the uranium deposit in Kvanefield is the world's sixth largest, 19 but experts suggest it only corresponds to less than 2% of the global annual uranium production. 20

A year later, on 7 April 2015, GMEL announced that a second MoU was agreed and signed with NFC. The second MoU stipulated that: a) GMEL would be responsible for finalising the exploitation license application to the Greenlandic government and commencing the permitting process; b) GMEL would complete pilot plant operations

in the coming months; c) NFC would provide assistance to GMEL in preparing the exploitation license application; d) Both parties would cooperate in identifying and completing further work programs required for the Project to reach bankable status.

It is worth mentioning that NFC's main interest appears to be on rare earth materials, with which a large amount of uranium is extracted as a by-product. Although China is now the world's largest rare earth producer, companies like NFC are always on the lookout for rare earth oxides to sell to their separation facilities in China.<sup>21</sup>

On 19 January 2016, Greenland and Denmark finally reached an agreement on how to cooperate on foreign, defence and security policy issues related to the mining and commercial export of uranium from Greenland.<sup>22</sup> On 1 February, the Danish Ministry of Business and Growth/Danish Business Authority (DBA) and the Greenlandic Department of Industry, Labour and Trade (DILT), released a joint declaration on export controls of dual-use items and technology. The declaration set out a framework for Greenland and Denmark to ensure "compliance with the Kingdom's international export control obligations in relation to uranium and all dual-use items."<sup>23</sup> 'Dual-use' refers to items such as software and technology that can be used in both commercial and military applications and/or as precursors or components of weapons of mass destruction; therefore, the declaration refers to uranium exports as well as the trade of all dual-use items in Greenland.

The Greenlandic Parliament followed this by passing four bills on 25 May 2016 to set up a regulatory and legislative framework that meets the Kingdom's international non-proliferation commitments. On 2 and 3 June, the Danish parliament passed legislation that creates a legal framework to allow Greenland to export uranium. The legislation states that Denmark assumes responsibility for the application of international safeguards to ensure peaceful use of Greenland's uranium. The legislation came into force on 1 July. With all these combined, Greenland now has the framework and regulations that allow the island to produce and export uranium while ensuring compliance with international treaties concerning uranium trade.<sup>24</sup>

On 23 September, GMEL made a surprise announcement that another major Chinese rare earth company called Shenghe Resources would acquire a 12.5% holding in GMEL and start a 'strategic working relationship'. Under the agreement, GMEL would receive \$4.625 million through the issue of 125 million shares priced at \$0.037 to Shenghe. Once the agreement becomes unconditional, Shenghe will have

the right to nominate a non-executive director to the board and will have anti-dilution rights to maintain a 12.5% position in GML.<sup>25</sup> Shenghe is engaged in the smelting, separation and deep processing of rare earths with a headquarter in Chengdu, China.<sup>26</sup> As mentioned earlier, Shenghe is mostly interested in rare earth materials, but with this agreement uranium extraction in Greenland will be for certain conducted by a company part owned by a Chinese enterprise.

#### HINKLEY POINT IN THE UK

The UK is the top European destination for Chinese FDI with 12 billion EUR between 2000-14.<sup>27</sup> China's FDI to Europe has been historically low, but has recently shifted the focus to services, thereby rapidly increasing investments to the UK in particular. Chinese companies tend to carry out sales and marketing operations or establish headquarters in the UK, mostly in the manufacturing sector followed by financial and business services. The UK is regarded as an ideal investment destination for developing knowledge and innovation as well as expanding market presence. Moreover, Chinese companies view London, which is home to more Chinese headquarters than elsewhere in Europe, as a gateway to Western markets.<sup>28</sup>

While the UK has been an advocate of a more liberal, less state-interventionist economy since Margaret Thatcher was prime minister, the so-called Brexit referendum on 23 June 2016 as well as a subsequent change of cabinet could change this direction. The vote to leave the EU is widely considered as an expression of popular disappointment with the elites and the workings of the liberal market economy advocated by Brussels. <sup>29</sup> Indeed, the new prime minister Theresa May has set up a ministry of "industrial strategy" and suggested the idea of adding more sectors to the list in which foreign takeover bids can be subjected to a "public-interest test". <sup>30</sup> At the moment, this is possible for defence, financial services and media companies.

The controversy regarding the Chinese investment in nuclear power in the UK centres on the Hinckley Point C nuclear power station in Somerset, England. The proposed site is one of eight sites announced by the UK government in 2010 to avoid an energy crisis in the mid-2020s when many of the existing nuclear plants reach the end of their lives.<sup>31</sup> On 26 November 2012, the UK government awarded a nuclear license to NNB Generation Company (NNB GenCo), which handled the bid to build new reactors and is owned by the French state-owned EDF (Électricité de France).<sup>32</sup> The new reactors, which were estimated to cost 14 billion GBP, were due

to start operating in 2023 if constructed on time and run for 35 years. It was calculated that the reactors would produce 7% of the UK's electricity, equivalent to the amount used by 5 million homes.

The Hinkley project caught media attention in October 2013 when the UK government and EDF finally made an agreement on the commercial terms of the project.<sup>33</sup> EDF announced that the company would build the nuclear plant with two Chinese nuclear companies, with EDF Group taking 40-50% shares, French AREVA 10%, and CGN in combination with CNNC 30 - 40%.<sup>34</sup>

The criticism at that time was focused on the fact that no British company would gain profit from this expensive project, to which the UK government was set to pay a massive amount of subsidy.<sup>35</sup> The UK and EDF had to seek for an investment from China because it was clear that EDF could no longer operate the Hinkley project on its own as the costs inflated from the original plan. This was due to unexpected issues with the AREVA European Pressurised Reactor (EPR), which was to be used for the Hinkley plant.<sup>36</sup> As it was a political project, UK and France had to avoid a deadlock.

Agreements between the UK government and EDF were for a long-term contract for the electricity generated at the Hinkley plant, which would have two 1600 megawatt AREVA EPR units, and for a guarantee for the project's debt.<sup>37</sup> The European Commission approved the agreements in October 2014. Under the Strategic Investment Agreement, signed in October 2015 in presence of the Chinese President Xi Jinping and the UK Prime Minister David Cameron, CGN agreed to take a 33.5% stake in the Hinkley project, as well as to jointly develop new nuclear power plants at Sizewell in Suffolk and Bradwell in Essex. Indeed, the Hinkley Point C project became the key investment of deals between the UK and China that was worth more than 30 billion GBP during Xi's official visit to the UK in October 2015.<sup>38</sup> Already years behind schedule, the Hinkley project has been given a revised start date.<sup>39</sup> In March 2016, the Commission approved the partnership between EDF and CGN for the development, construction and operation of three new nuclear power plants in the UK including the Hinkley Point C project.

Around the time of Xi's visit to the UK, critics began to raise security concerns about allowing Chinese nuclear companies to build a nuclear power plant as part of UK's critical national infrastructure. In particular, the involvement of the second Chinese nuclear company CNNC, which was set to supply its engineering expertise to the project, was considered problematic. As mentioned earlier, CNNC is a state-owned

enterprise directly under the Chinese central government. Although CNNC now specialises in nuclear power and uranium exploration, it has a track record of developing atomic bombs, hydrogen bombs and nuclear submarines since its foundation in 1988.<sup>40</sup> Combined with the fact that the government investment in a large-scale, risky nuclear plants goes against the industry trend of moving to renewable energy, one British critic called the Hinkley Point C project with China as "one of the maddest ever struck".<sup>41</sup>

A further delay of the project began to pose a serious threat to the financial stability of EDF. Already in October 2015, rating agencies said EDF would lose its credit rating if it took the lead in the UK projects without proposals; in response, EDF announced that it planned to sell as much as 10 billion EUR worth of assets over the next five years. <sup>42</sup> In June 2016, senior figures of EDF told the UK parliament's energy and climate change committee that the Hinkley project should be postponed, until it has "solved a litany of problems", including EDF's soaring debts and reactor design problems. <sup>43,44</sup> Although publicly denied, it is rumoured that CGN has considered an independent plan to build reactors without EDF, if/when it should decide to withdraw. The situation regarding the Hinkley C project suggested a possible future of UK's major nuclear power plant almost fully designed, built, managed and owned by Chinese state-owned nuclear companies. <sup>45</sup>

There will be reforms to the government's approach to the ownership and control of critical infrastructure to ensure that the full implications of foreign ownership are scrutinised for the purposes of national security.

On 29 July, EDF announced that it had a board meeting and the board narrowly voted to approve the Hinkley scheme. However, almost immediately after this, Greg Clark, Britain's new Business and Energy Secretary, announced that ministers would once more review the project. He project would further be delayed, as it needs a final approval from the UK government in order to proceed. It was reported that the reasons behind the renewed review of the Hinkley project were: a) the new UK prime minister Theresa May would like more time to study the project, b) May has doubts about China's involvement in an important domestic project. The renegotiating of costs, d) the possible use of the review as a negotiation tactic for Brexit as UK looks for leverage with France, and e) the scrapping of the expensive project without losing anyone's face.

In response to UK's deferral of the Hinkley project, China reacted strongly. Its ambassador to London Liu Xiaoming published an article in the Financial Times stating that the China-UK relationship was at a crucial historical juncture and that the deferral imperilled the relationship. He urged London to approve Hinkley as soon as possible and expressed a hope that "the UK will keep its door open to China".<sup>49</sup>

In mid September 2016, Theresa May approved the Hinkley project, but with the condition that EDF will not sell its stake in the plant during construction and the government would take a "golden share" in future nuclear schemes. This latter measure appeared aimed at addressing Mrs May's security concerns over plans by CGN to take the lead in the construction of further reactors at Bradwell in eastern England, using Chinese technology. The UK government also stated: "There will be reforms to the government's approach to the ownership and control of critical infrastructure to ensure that the full implications of foreign ownership are scrutinised for the purposes of national security." 50

### NON-WESTERN COUNTRIES: PAKISTAN, SAUDI ARABIA, IRAN AND UKRAINE

Like its previous adventures in telecommunications and white goods, China tries to export its nuclear technology in the developing world first, building experience and reputation, before it enters developed markets. Developing countries often have a more relaxed regulatory environment than Western countries over nuclear power. So far Pakistan has received most of Chinese investment in nuclear power and is the only country with Chinese-built nuclear plants under operation.

#### **Pakistan**

Pakistan is an 'all-weather strategic partner' of China, always made as a flagship example of benefiting from China's economic diplomacy, including enjoying the early harvests of a free trade agreement, signing bilateral currency swap arrangements, and hosting the China-Pakistan Economic Corridor that is a crucial part of China's most important One Road One Belt initiative. It is also the country that has received the highest number of Chinese-invested nuclear projects, and China regards Pakistan as a flagship for demonstrating the reliability and benefits of Chinese nuclear technology. In August 2015, the first project that uses China's latest Hualong-1 technology started construction in Karachi in Pakistan.

CHINA'S OVERSEAS INVESTMENT IN CRITICAL INFRASTRUCTURE

The US's considerations of political expediency and business interests have in the past accommodated or turned a blind eye to China-Pakistan nuclear cooperation. China was allowed membership to the Nuclear Suppliers Group (NSG)<sup>51</sup> in 2004 despite supplying two nuclear power stations to Pakistan, even though Pakistan is not a member to the Non-Proliferation Treaty (NPT). That was because the US had just set a precedent of giving India wide exemption from being banned from receiving nuclear investment, and the US needed the political expediency of getting China's support on sanctions on Iran. In June 2016, however, China, together with New Zealand, Ireland, Turkey, South Africa and Austria, blocked India's bid to join the NSG, which was supported by the US.

The next two Chinese invested nuclear stations in Pakistan caused concern among NSG countries and within some circles in the US because China only got exemption for building the first two plants in Pakistan from NSG. Pakistan caused worries among NPT members that it indiscriminately supplied nuclear technology and materials to countries like Iran, North Korea and Iraq. One of Pakistan's nuclear scientists and black market organisers, Abdul Qadeer Khan, admitted in 2004 his dealings with these countries of transferring nuclear secrets. It is widely suspected that his operations were supported by the Pakistani government, though the government denies it. American nuclear companies, however, still seeks access to the domestic Chinese market. In response to doubts of supplying China with nuclear technology at the risk of being copied by China, the US companies and lawmakers argued that they would help China set high safety standards rather than leaving the opportunity to other countries.

Now China is even building two more nuclear plants in Pakistan, using the latest technology that China has to date and has only begun to build demonstration plants within China. In 2013 China committed to provide \$6.5 billion in financing for the construction of a nuclear power plant by CNNC in Karachi in Pakistan, scheduled to be completed in 2019. Each of the plant's two reactors will provide more power than all of Pakistan's current nuclear reactors combined. The Karachi project in Pakistan is therefore part of China's diplomacy as well as demonstration and experiment of its nuclear technology.

#### The Middle East

There is a civil nuclear race in Middle East, as countries in this region seek to expand their domestic nuclear energy supply and many have turned to China, Russia and Japan. The Arab States of the Persian Gulf plan to start their own joint civilian nuclear programme, and Iran is grasping the newly opened opportunities after it reached a nuclear deal with major countries in 2015.

China plays a pragmatic and active balancing game among the regions' rivals, seeking to sign contracts not only with Iran but also with Saudi Arabia, Egypt, Jordan and Turkey. China has also sought to sign a Memorandum of Understanding (MoU) with Egypt to cooperate in the construction of nuclear power reactors. In 2015, China and Jordan agreed to strengthen their nuclear cooperation. China is also cooperating with Turkey for construction of nuclear power plants for Turkey. Saudi Arabia and Iran are arguably the most important cases.

#### Saudi Arabia

Saudi Arabia has been China's top crude oil supplier for almost ten years, while both countries seek to expand their energy sources to nuclear power. Saudi Arabia plans to construct 16 nuclear power reactors over the next 20 years at a cost of more than \$80 billion, with the first reactor on line in 2022 to be built by China. It has signed nuclear cooperation agreements with France, Argentina, South Korea, Russia, Hungary and China, and it is in talks with UK, the Czech Republic and the US regarding further cooperation.

Saudi Arabia has been a friend of the US in the Middle East, though it now seeks to have closer relations with China as well. In the 1990s and 2000s, anecdotal reports speculated that Saudi Arabia received assistance from Pakistan in developing nuclear weapons, and in turn financed Pakistan's nuclear programme. However, it has signed an agreement with the US in 2008 to boost Saudi efforts for a civilian nuclear programme, as part of the US Atoms for Peace programme.

During his Middle East tour in January 2016, Xi Jinping signed agreements with both Iran and Saudi Arabia on nuclear cooperation. China committed to invest \$2.43 billion to build a nuclear manufacturing equipment industrial cluster in Saudi Arabia, while underlining the latter's important position at the west crossroads of the grand Belt and Road initiative. KA-CARE, Saudi Arabia's nuclear energy agency, signed an agreement with China Nuclear Engineering Corporation (CNEC) to build a high-temperature reactor, based on China's indigenous fourth-generation technology, now under construction in China by CNEC. CNEC hopes that the agreement with Saudi Arabia will bring other possibilities for nuclear cooperation between China and other partners along the Belt and Road routes.

Saudi Arabia has been an opponent of nuclear weapons in the Middle East. It has signed the Nuclear Non-Proliferation Treaty, and is a member of the coalition of countries demanding a Nuclear-Weapon-Free Zone in the Middle East. However, it has stated that it would consider making nuclear weapons if Iran obtained them too.

### Iran

China views Iran as an important source of energy and a counterforce to Western influence. China has had nuclear cooperation with Iran since the 1980s, when it reportedly exported uranium, research reactors and laser enrichment equipment to Iran, which was used by Iran for testing parts of a uranium conversion process. China officially cut off nuclear ties with Iran during the nuclear impasse, but covert cooperation was suspected by Western countries. In 2005, seven Chinese firms were suspected of selling nuclear weapons technology, and all seven were thus banned from trading with the US for two years.

China, together with Russia, endorsed UN sanctions against Iran's nuclear programme in 2010, as Beijing does not wish either Iran or North Korea to possess nuclear weapons. At the same time, China has worked hard within the P5+1 group (the UK, China, France, Russia and the U.S.+ Germany) to reach a nuclear deal with Iran to allow the latter to develop a civil nuclear programme. After the deal was reached in 2015, other countries are allowed to help Iran develop its civil nuclear programme for peaceful purposes. Several countries have since competed for the Iranian civil nuclear market, including China, Japan, South Korea, Russia and Spain. CNNC has signed an agreement with Iran in July 2015 to build two plants at the Makran coast. Compared with Russia, which signed an agreement with Iran in November 2014 to construct simultaneously eight plants in Iran, China's nuclear export to Iran is less significant. It however provides Tehran with an alternative and leverage over Moscow.

With the sanctions being allowed to be gradually lifted after IAEA ruling in January 2016, bilateral relations between Beijing and Tehran have even more room to flourish, including Iran's membership at AIIB and potential membership at the Shanghai Cooperation Organization, as well as its role in China's One Belt One Road grand initiative. During the January 2016 visit of China's President Xi Jinping, Iran's President Hassan Rouhani announced that the two countries plan to build economic ties worth up to \$600 billion, with cooperation on peaceful nuclear energy as an important item. Tehran announced that it would take help from China on reconfiguration of the Arak nuclear facility.

#### Ukraine

China has been expanding its political influence and economic opportunities in Central Asia as part of the grand OBOR initiative. Chinese companies have been seeking opportunities in gas, coal gasification and automobiles. Nuclear power is a new field for China in Central Asia.

Ukraine, traumatised by the Chernobyl disaster in 1986, has so far worked with Western countries to upgrade its existing nuclear reactors. It is, however, now also looking to China to provide nuclear support.

Two months before he was ousted, the Ukrainian president Viktor Yanukovich signed an agreement with Chinese President Xi Jinping during his visit to Beijing in December 2013. It reportedly amounted to \$10 billion and included an "unusual" nuclear clause: in the event of a nuclear attack or the threat of one, China would offer Kiev military support. <sup>52</sup> In practice, China has kept out of the conflict between Ukraine and Russia so far. It has not expressed support to Russia, but it has also been careful to refrain from criticising it.

Chinese companies are interested in the upgrading of existing and construction of new nuclear capacities in Ukraine. <sup>53</sup> In July 2015, Ukrainian Nuclear Fuel and China Nuclear Energy Industry Corporation (CNEIC) signed a memorandum on cooperation in the field of a nuclear fuel cycle. In May 2016, they began talks on a \$600 million investment in uranium mining in Kirovohrad region in Ukraine.

#### **DISCUSSIONS ON NUCLEAR POWER**

China is building a large number of nuclear plants within its borders and is 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. They have learned Western technology in the past three decades from collaborating with them on domestic plants, and now they are developing and building indigenously designed reactors and trying to export them overseas. Their overseas investments are 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 the Middle East, Central Asia, Africa and Europe. In particular, China prioritises countries along the One Belt and One Road, which is the most important foreign policy strategy of the current government. With Western companies downscaling their activities due to economic slowdown, Chinese nuclear investment offers an

attractive alternative, in particular to developing countries, because of its large capital and competitive price. There is, however, still a question of economic safety, as nuclear projects are all very expensive and can be a heavy burden on the host country, or as the Western company that is partner in a project may not be able to carry through due to financial troubles.

In terms of nuclear safety, China prides itself in having built and run many reactors domestically, but its overseas record is limited. China's involvement in overseas nuclear projects has mainly been contributing capital and construction workforce, to match with Western design. However, it has started to export its own technology, with two nuclear plants under construction in Pakistan and more contracted with other countries, with the intention of demonstrating the safety of China-built reactors to the world. Because China is using its latest technology in building nuclear plants overseas and domestically at the same time, it is too early to judge their safety. Moreover, the rapid development is taking place despite a recent Chinese official document pointing out insufficient safety control measures or disaster response programmes within China.

The government now does not wish either Iran or North Korea to possess nuclear weapons.

As for nuclear proliferation, China is a member of the NPT and the Nuclear Suppliers Group. It is suspected to provide nuclear technology to Iran, North Korea and Pakistan in the early years of the Communist regime, but the government now does not wish either Iran or North Korea to possess nuclear weapons. Beijing encourages a peaceful nuclear programme in Iran after the latter had reached a nuclear agreement with major powers in January 2016, getting international sanctions gradually lifted. China's export of nuclear technology to Pakistan, however, raises international concerns because Pakistan was the source of proliferation in the early years despite the government's denial of involvement. Even though the international community allowed China to build the first two plants in Pakistan as a counterweight to US help with India's nuclear programme, now China is going beyond this exemption and the risk of proliferation depends on how Pakistan and other countries, like Iran, use their newly obtained technology.

For Western countries, China is an important market for their nuclear companies. 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 of government and another round of security reviews. More caution is expected in other Western countries, too, towards Chinese nuclear investment, as nationalism and protectionism are on the rise, while the governments are not certain about the security or strategic implications of letting Chinese nuclear companies into this critical sector.

How much China can tap into the rare earth resources in Greenland depends on the interpretation and application of the new rules.

The same could be said about uranium and rare earth export to China, the area where China has a major interest in Greenland. The Greenlandic government has in the past several years been interested in inviting Chinese investment in mining rare earth that contains uranium, and the Australian company operating in Greenland has signed MoUs with a major Chinese state-owned enterprise on exploitation and is scheduled to be partially owned by another Chinese company. The new agreement between Greenland and Denmark in 2016 will put more checks on the export of uranium and rare earth to China. Therefore, how much China can tap into the rare earth resources in Greenland depends on the interpretation and application of the new rules. If China is hindered by the new rules, the Chinese government and companies are likely to regard it as an unfriendly gesture from Denmark, and with it could come economic and foreign policy implications, even though uranium from Greenland would still make a small portion of China's demands for its ambitious nuclear programme at home and abroad.



## **SCANDINAVIA**

After some latency in breaking into the Scandinavian telecommunications markets and critical infrastructures, Chinese involvement (or, more precisely; Huawei, who continues to have by far the largest presence) has been rapidly increasing here over the last decade. Compared to the African markets, the entrance into Europe was slow, likely held back by widespread suspicion and bans in the US, Canada and Australia, where Huawei is still not allowed to bid and contract government entities. Sale of telecommunications hardware to Scandinavian consumers has nonetheless skyrocketed over the last few years, and involvement in critical infrastructures was genuinely ignited when in 2009 Norwegian tele-giant Telenor publicised that Huawei had been tasked with setting up the country's 4G network, a deal worth approximately \$150 million. Today, the company has in the neighbourhood of 1.000 employees in Scandinavia, and more than 10.000 in Europe.

## **Huawei in Denmark**

Among the Scandinavian countries, Denmark undoubtedly hosts the strongest Chinese presence in telecom markets and infrastructures. Huawei's presence in the market here is increasing with great haste since Huawei established a DK office in 2007. In 2015, Huawei's sales of smartphones rose by 60%, and in the last two months of 2015 it was the third bestselling smartphone company in Denmark, only passed by Apple and Samsung, corresponding to its contemporary global position as the world's third largest smartphone producer. Since entering into the Danish market with budget models and 3G dongles a decade past, Huawei is increasingly selling high-end smartphones and its brand awareness in Denmark rose by 69% in the last evaluation in 2015. Huawei's Danish division counts more than 250 employees, of which approximately 60% are Danes, the greatest part of the rest Chinese, but with a total of at least 21 nationalities represented.

The company's titanic breakthrough into Danish critical telecommunications infrastructure came in 2013, when TDC, the largest Danish telecommunications company, signed a deal with Huawei worth \$700 million to change all of its base stations in Denmark and ensure 99% of the Danish population access to high speed internet access by 2015. TDC has roots back to 1879 but was legally formed in 1990 (as Tele Denmark) when the Danish Parliament decided to merge different public regional telecom companies into one national. Up until 1996, TDC enjoyed monopoly of the Danish telecom market as the sole public provider, and in 1998 the Danish state's involvement was finalised as TDC became completely privatised. Chinese

involvement in Danish critical infrastructure thus forms part of a larger narrative of Danish privatisation occurring in the 90s and 00s, the consequences of which were probably not fully understood.

In 2015, a documentary made by the Danish Broadcasting Corporation (DR) posed a series of substantial accusations against Huawei and their involvement with the NOC.

Swedish Ericsson had been tasked with maintaining TDC's network since 2008 when rumours of Huawei potentially overtaking the future service of the network surfaced in the summer of 2013. Despite little insight (or perhaps exactly because of this), the public reaction was quite substantial, and the deal was an object of extensive public debates in the Danish press and in Parliament, where the apprehension mainly seems to have concerned security concerns of letting a Chinese company, accused of espionage but still legally innocent, gain access into the heart of Danish telecom infrastructure, more so than neglecting business with a neighbouring country (Sweden). The same apprehension seems to have been present in the Danish Defence Intelligence Service (DDIS), who, according to Danish newspaper Politiken, had prepared an internal report already in 2011, which warned against the entrance of Chinese telecom giants into Danish critical infrastructure. Later, however, DDIS changed its mind, as the 2013 disclosure of the TDC and Huawei deal was followed by a press statement in which the Center for Cyber Security (CFCS, an institution under DDIS) made it clear that it had followed the deliberations concerning the deal and an agreement was made that: allowed CFCS to monitor Huawei's work with TDC's network; only allowed individuals with security clearance to work in the so-called Network Operation Center or NOC, from where TDC's network is controlled; and would require all to-be installed Huawei hardware to go through a screening in a department of the company referred to as 'The Cell' (its official name is CSEC) in the UK, where security experts cleared by the UK check all Huawei equipment to reveal any issues backdoors and similar security-compromising soft- and hardware (despite its somewhat independent status from Huawei, a report to the British parliament found that The Cell largely remains a case of 'self-control' more so than proper independent control).

As it would later turn out, this deal was voluntary in nature as CFCS did not have mandate to monitor when it saw fit, and an extension of CFCS authority would later be introduced by parliament as part of the Danish Government's 2014 (December)

national strategy for cyber and information security. In concluding the deal, Huawei representatives stated that the security measures where even greater than in its British deals, that it followed ISO27001 and that 'No data is transferred to China'.

In the fall of 2013, then, the deal worth \$700 million was publicised. Huawei was to update and maintain (for the following six years) Denmark's largest mobile network, affecting 70% of the Danish population or 3.3 million people, including public institutions like the Danish parliament and ministries. All base stations in the mobile network were changed by Huawei and a Network Operation Center (NOC) was established in Copenhagen (TDC thus transferred some of their network control which had functioned from Romania until then), in which TDC and Huawei employees were to work alongside each other. As a rare occurrence, quality was written into the contract that obligates Huawei to deliver the best Danish network, a feat it thus has to continuously measure and prove.

In 2015, a documentary made by the Danish Broadcasting Corporation (DR) posed a series of substantial accusations against Huawei and their involvement with the NOC. They found several instances of non-security-cleared individuals working within the NOC, the gravest of which in march 2015, where 35 Huawei employees worked in the NOC without security-clearance. CFCS defended the case and explained that the security-clearance process is extremely longsome (taking up to 6 months) and that they had granted a wish for Huawei employees to work without clearances as long as they were monitored by someone with a security clearance. TDC responded to the accusations with claims that Huawei employees do not have access to information concerning SMS, calls and e-mails that are all situated outside the reach of the company's employees. They maintained that Huawei employees, accordingly, do not have access to personally sensitive data, and that only a few people with the highest security clearance in TDC has that, but also that all activities in the network are logged (as per the security agreement between TDC, Huawei and CFCS).

The commercial engagement between TDC and Huawei does not seem to slow down, quite the opposite. In January of 2016, Huawei announced that it was partnering with TDC to upgrade the company's coaxial network, starting in the summer of 2016 and expected to be completed by the end of 2017, making Denmark the country to upgrade an entire cable network to so-called 'Giga COAX', which offers 1gps connectivity. Head of TDC group, Pernille Ernebjerg, announced that '[i]t is the most ambitious and comprehensive upgrades we have ever made in our cable network and at the same time it is one of the largest investments in digital infrastructure we have seen in Denmark'.<sup>54</sup>

Ultimately, Huawei's involvement in Danish telecom is a complex matter of national security vis-à-vis trade and potential economic growth through increasing financial relations to China. Likewise, in a hearing in the Defence Committee in the Danish Parliament, Huawei representatives told Danish politicians that they were afraid national security concerns or cyber security could work too much as barriers of trade. It seems that commercial concerns have largely taken the upper hand in this deal. On the other hand, as much as a lot is at stake for Denmark in having to balance economic concerns with national security, any real evidence of industry or otherwise strategic surveillance or espionage by Huawei would likely ruin the company's engagements in Europe.

## **Huawei in Sweden and Norway**

As in Denmark, Huawei opened its doors in Norway in 2007, back then with 7 employees but growing to more than 140 today. Huawei won a Telenor bid to build a 4G mobile network in Norway in 2009, ahead of Ericsson and Nokia Siemens Network. As one of the biggest LTE deals in Europe, it was worth approximately \$120 million over five years. Huawei became Norway's biggest telecoms supplier in 2010 through its deal with Telenor, and subsequently entered the Norwegian mobile phone market in 2011. The 4G network finished construction in October of 2012, and it was not until then that the Telenor-Huawei deal became an object of public discussion, also coinciding with Huawei's testimonies to the US congress and the release of the report to the US Permanent Select Committee on Intelligence questioning the motives of Huawei through its perceived relations to the Chinese state. Some politicians were apprehensive of Huawei entering Norwegian critical infrastructures<sup>55</sup>, but the government was largely defensive of the choice of Huawei and considered the accusations exaggerated, underlining that the Norwegian Communications Authority is tasked with monitoring Norwegian networks and thus also expected to monitor Huawei's involvement. Opposite e.g. Denmark's approach to Huawei's involvement, the Norwegian authority does not require equipment to be screened before it is installed. By 2015, Huawei had annual revenue of almost \$100 million in Norway, with the carrier business accounting for 70%, consumer products for 25% and the corporate market for just the remaining 5%.

While the biggest Huawei deals have been made in Denmark and in Norway, Sweden remains the Scandinavian country with by far the greatest Huawei involvement as per employees and diversity of commercial engagement. It is also where the by far biggest Scandinavian (and globally in terms of mobile telecoms equipment) competitor to Huawei, Ericsson, resides. Founded in 1876 and headquartered in Stockholm, Sweden, Ericsson has more than 110.000 employees worldwide, and

generated a revenue of SEK 246.9 billion in 2015 (approximately \$30 billion). Huawei engagement in Sweden started in 2000 with the establishing of a research and development centre in Stockholm, not far from Ericsson, with the purpose of designing a 3G system, recognising that expertise pertaining to this technology was to be found in Europe more so than at home in China. Around 350 people work at this facility today.

From 2006-2009, Huawei mainly delivered USB modems to Telia, Tele2, and Telenor. In December of 2009, however, Huawei won a bid when the Telenor/Tele2 joint venture Net4Mobility decided to hire the company to provide LTE kits in Sweden. The deal was won ahead of Ericsson who was so disappointed that a press statement was released explaining that the Swedish company could not compete with Huawei on prices<sup>56</sup>. In 2010, however, TeliaSonera announced Ericsson (and Nokia Siemens Networks (NSN)) as the company to provide its LTE equipment. In 2015, Huawei announced that it would be hiring a further 100 employees to work on Research and Development in Sweden. In comparison, Ericsson during that same time announced that 2200 positions were to be determined. Today, Huawei has more than 600 employees in Sweden, with at least 350 engaged in research and development activities in its offices in Lund, Stockholm and Gothenburg. Some questions have been raised over the working environment and organisational culture in Huawei's Scandinavian offices, and in 2011, Sweden's national radio (Sveriges Radio), reported widespread harassment, threats and public punishment of Huawei employees by senior staff, based on interviews with 20 anonymous current and former employees.<sup>57</sup>

#### NOT SO SUCCESSFUL ATTEMPTS TO ENTER THE US

The two biggest Chinese telecommunications manufacturing companies, Huawei and ZTE, have been banned from bidding for US government contracts, because of worries that they might undertake industrial and strategic espionage for China. As mentioned earlier, ZTE is state-owned, while Huawei's founder, Ren Zhengfei, had served in the Chinese army before he started the company in 1987.

In February 2011, Huawei published an open letter to the US Government denying security concerns and requesting a full investigation into its corporate operations. After a year of investigations and hearings, the US House Intelligence Committee concluded in 2012 that Huawei and ZTE 'cannot be ruled out to be free of foreign

state influence'. Crucial evidence in this report was classified information provided by National Security Agency (NSA). The US congressional report recommended that the country's telecom operators avoid using equipment made by Huawei and ZTE for security risks.<sup>58</sup>

Both companies have denied that their equipment permit any backdoor surveillance, but they became subject to increasing scrutiny in the EU, India, Australia, Canada, South Korea and other countries that shared security interests with the US, not least because of US pressure.<sup>59</sup>

Only days after the Congressional report, Reuters disclosed that the White House had ordered an 18-month review of security risks posed by suppliers to US telecom companies. It found no clear evidence that Huawei Technologies had spied for China, but pointed to vulnerabilities in Huawei's networks that hackers could exploit in the future.<sup>60</sup>

In March 2016, the US briefly blocked sales of American technology to ZTE because of allegations that ZTE had violated American export sanctions by selling US-made products to Iran. ZTE responded quickly to pledge cooperation with US officials, and the sanctions on ZTE were lifted on a temporary basis after only two weeks. ZTE later also removed its chief executive and two other top company officials to demonstrate compliance.<sup>61</sup>

Ironically, the US investigation into the possible link between Huawei and the Chinese military has adopted espionage methods and become part of the cyber war between the two countries.

In a bigger step, in June 2016, the US Department of Commerce issued a subpoena to Huawei demanding that the company turn over all information regarding the export or re-export of American technology to Cuba, Iran, North Korea, Sudan and Syria, which would be a breach of US export controls. For example, in September 2015, Huawei signed an agreement with Syria's Communications and Technology Ministry to help the country develop its communications networks. If the investigation finds that Huawei was acting counter to US national security or foreign policy interests, it could limit the company's access to crucial American-made components

and other tech products. This would affect Huawei's network and infrastructure projects around the world because many of Huawei's products use American components or work with American technology.

Ironically, the US investigation into the possible link between Huawei and the Chinese military has adopted espionage methods and become part of the cyber war between the two countries. In 2014, The New York Times and Der Spiegel disclosed that NSA had infiltrated the servers of Huawei's headquarters and monitored Huawei for at least seven years, according to documents provided by former NSA contractor Edward Snowden. NSA was looking for links between Huawei and the Chinese military PLA, but the plan, code named 'Shotgiant', went further: to exploit Huawei's technology so that when the company sold equipment to other countries, the NSA could roam through their networks to conduct surveillance and even offensive cyber operations.<sup>62</sup>

In short, the US investigation of Chinese telecom companies' link to the Chinese government, probably the most thorough in the world so far, has not revealed any non-classified information that indicates an intentional collaboration to obtain US intelligence, but the US government warns against their security risks anyway. This case also shows that in the process of investigating Chinese companies' connections to Beijing, host country governments run the risk of violating laws and conducting espionage. At the same time, the US and other countries have the capacity and possibility of intruding into other countries' information network as well.

## CHINA'S INVESTMENT IN TELECOMMUNICATIONS: UK

According to a list of Chinese companies in the UK by the UK Trade & Investment, there are eight Chinese telecommunications companies, of which Huawei and ZTE are the two biggest.<sup>63</sup>

Both companies opened their first offices in London in 2001. In 2016, Huawei has 15 offices across the UK and over 1,100 employees.<sup>64</sup>

Huawei's investment in the UK became an issue when BT, a British telecommunications services company formerly owned by the British government, awarded Huawei the contract to supply some of the transmission equipment in December 2005. In January 2006, the UK Intelligence and Security Co-ordinator wrote to the

Home Secretary to seek agreement to assist BT to monitor Huawei's work upon BT's request. This was the first time that the British Ministers were made aware of the security concerns of using Huawei's technology in UK's Critical National Infrastructure. <sup>65</sup>

The UK government raised concerns about Huawei equipment with Huawei UK, and proposed the establishment of a security centre.

After a few years of investigation, in February 2010, the UK government raised concerns about Huawei equipment with Huawei UK, and proposed the establishment of a security centre. The Cyber Security Evaluation Centre (called the Cell) was launched in November within Huawei in Banbury. The Cell is funded entirely by Huawei and staffed by security cleared UK personnel. Its function is to test all updates to Huawei's hardware and software for high-risk components before they are deployed on UK networks, not necessarily to find every single vulnerability but to reduce the risk of using Huawei equipment "to a similar level to that of established manufacturers" including large suppliers from the US. Meanwhile, in June 2013, the Intelligence and Security Committee of the UK Parliament released a report raising concerns about the central role of Huawei in Britain's telecommunications infrastructure. The report provides details of how Huawei came to supply equipment to BT and criticised the attitude of the British government to have turned a blind eye to potential security risks in working with a company like Huawei for the sake of financial benefits or to avoid jeopardising future Chinese investment.

Despite the release of the report and extensive media coverage, however, the British government continued to rigorously promote Chinese investment in the UK, Huawei being one of the prime examples. This is largely due to then-chancellor George Osborne and his so-called "Osborne Doctrine", in which he hoped China to become the UK's second-largest trading partner by the end of 2025. In May 2016, Huawei announced that it concluded a three-year MoU with the UK Trade & Investment (UKTI) to "identify the best UK technology partners for Huawei's global supply chain and support Huawei's investment and business development in the UK." On 28 June, it was reported that Huawei would continue with its planned investment in the UK worth 1.3 billion GBP (1.73 billion USD) despite the UK's vote to leave the European Union. However, as seen in the case of the Hinkley Point C nuclear power

project mentioned earlier, it would not come as a complete surprise if the current prime minister Theresa May intervenes with Huawei's plans in the UK over security concerns. Indeed, the new National Cyber Security Centre is scheduled to open in November 2016.<sup>72</sup> The new centre will focus on conducting cyber defence operations to improve the UK's protection from digital attacks and providing assistance to public and private sector organisations to improve their cyber security.<sup>73</sup>

# CHINESE INVOLVEMENT IN AFRICAN TELECOMMUNICATIONS INFRASTRUCTURE

In December of 2015, Xi Jinping offered a \$60 billion loan and aid package to Africa with the aim of developing infrastructure and reducing poverty. Among the types of infrastructure, media and telecommunications (or ICT) is one of the fastest growing and most significant. From 2005-2012, the telecommunications sector represented 34% of all Chinese investments in Sub-Saharan Africa, second to only transport.

The mobile industry, the specific form of ICT in focus here, is also growing fast with Sub-Saharan Africa reaching 367 million subscribers in mid-2015, driven equally by economic growth and falling device prices. The region is expected to add 400 million new smartphone connections by 2020, with half the population expected to hold subscriptions by then. Africa in its entirety is now the world's second-largest market, second to Asia

African telecommunications is an arena of great competition as also European (Vodafone) and Indian (Airtel) companies are seeking influence and market share. In this context, Chinese involvement in African critical infrastructure surrounding ICT has been increasing at a rapid pace over the last decade already, not least with Huawei and ZTE as the two central drivers of Africa's mobile revolution. Huawei alone has been engaged in African telecommunications since 1998, where it entered the Kenyan market, and now has 16 country offices and its headquarters in Johannesburg, South Africa. Huawei has penetrated almost every telecommunications market on the continent, and has opened up seven training centers and a Research & Development facility.

Examples of Chinese investments in telecom include Huawei and ZTE landing more than \$1 billion in contracts with Nigerian Globacom, and Huawei's selection by Kenya's leading operator (Safaricom, partially owned by Vodafone) as the sole

constructor of its fibre optics network. Especially the valuable cheap smartphone market is dominated by Chinese companies including ZTE, Huawei, Gionee, and Xinwei, which launched smartphones in the sub-\$20 range in mid 2015. Perhaps unsurprisingly, private investments alone have not facilitated the Chinese dominance. The Chinese National Development Bank (CDB), the China Exim Bank and other national banks have been important facilitators securing the increasing market-share of Chinese telecommunications in Africa. Huawei and ZTE alone are found to have received \$45 billion in authorised export credits (essentially loans to the company's foreign customer) from CDB alone. However, one should not equate strong Chinese involvement with a unitary state led by one mind, in which all Chinese companies follow orders form Beijing. Huawei, for instance, has taken ZTE to court over a case of who had the right to provide Kenyan police with communication and surveillance technology in a significant deal.

The Chinese dominance of backbone telecommunications systems all over Africa gives quite some potential for insight into fundamental channels of communication.

The repercussions of Chinese involvements extend far beyond immediate commercial concerns for European companies and carry with it significant political and security-related implications. The wider Chinese media and communication strategy in Africa cuts across almost all types of ICT including television (with the launch of CCTV Africa in 2012, by then the largest non-African TV initiative in Africa), radio (China Radio), newspapers (China Daily and its Africa Weekly edition). These often emphasise 'positive reporting', i.e. no negative news on Chinese engagement in the region, and exercise tight control over controversial issues on human rights and the environment (Galiardone & Geall, 2014).

Moreover, the Chinese dominance of backbone telecommunications systems all over Africa gives quite some potential for insight into fundamental channels of communication. We do not know the extent to which such control over and interception of information is used in Beijing, but in the national contexts, it is widely used by leaders for political purposes. The following case of Ethiopia illustrates the problematic influence of Chinese involvement in African telecommunications, but should of course be nuanced against similar practices by European and American companies.

## **Chinese involvement in Ethiopian telecommunications**

Unlike the vast majority of other African countries, Ethiopian telecommunications is completely closed with one operator, Ethio Telecom (formerly ETC), and all telecommunications investments are made under the auspices of the government. Chinese companies, especially ZTE and Huawei, have been involved at least since 2003 in building up Ethiopia's telecom infrastructure. In 2006, ZTE, Huawei and China International Telecom Corporation (CITCC) signed contracts worth \$2.4 billion as the Ethiopian government took steps towards modernising its outdated infrastructure. The same year, ZTE won the exclusive rights to become the sole equipment vendor for the ETC, mainly because of its backing from the CDB who facilitated a \$1.9 billion loan to the Ethiopian government. By then, only 500.000 Ethiopians had mobiles. Today, that number is well beyond 20 million. In 2013, ZTE and Huawei won a bid to further expand mobile and internet connectivity, amounting to \$1.6 billion.

With the technology provided to them from especially Chinese companies, Ethio Telecom has the ability to access any phone call or text message from any phone in Ethiopia, just as it can shut down parts of the network and has done so at sensitive times during elections, protests and whenever it has perceived a threat. According to some, this has allowed the Ethiopian government to maintain strict control over internet and mobile technologies to monitor and limit information communicated and accessed, curtailing freedoms of expression and association (HRW, 2014). ZTE has, as an example, developed a 'customer management system' called ZSmart. Text messages or conversations can easily be searched for and downloaded to a USB stick, almost by any employee of Ethio Telecom, without any form of judicial warrant (HRW, 2014). Knowledge of calls may be suitable for business and customer management, but the access to recordings and content of text messages is a completely different level of surveillance.

The ability to monitor calls and texts is not unlike what most governments in the world have the technological capacity to do. The problem here, as elsewhere under similar conditions, of course lies in the fact that no judicial or legislative mechanisms are in place to protect privacy and other rights, preventing such instances from happening. This is of course first and foremost a problem of the state in question and its authoritarian predispositions. But the mode of cooperation and business of Chinese companies, and especially their heavy preference for state cooperation, combined with the EPRDF's ties to the CCP (which seem to be strong), exacerbates and supports these troubling authoritarian practices.

### **DISCUSSIONS ON TELECOMMUNICATIONS**

Telecommunications is a commercial area that has seen widespread privatisation and outsourcing of services and technical equipment over the last decades, and especially Western countries have now privatised formerly state-owned entities. Accordingly, the logics of operation are gradually shifting from nationally- and stability-focused to short-term profitability and private investments. This leaves open a space for involvement for companies able to offer appropriate technology and services at a commercially competitive level.

Across the cases accounted for in this part, Chinese involvement differs greatly from issues of intensity and depth of engagement to host-country perception of the involvement. In the US, both ZTE and Huawei are banned from bidding for government contracts, and can neither be used as subcontractors for pieces of equipment because of continued worries over industrial espionage. In the UK, the commercial engagement of especially Huawei is extensive, and it was here that the company's Cyber Security Evaluation Centre (the Cell) was established to screen Huawei equipment. The Cell is also used to service other countries such as the Scandinavian ones, where especially Huawei involvement continues to grow (ZTE appears to not have the technological edge to enter into more advanced markets).

Across these Western contexts, Chinese involvement in national telecom infrastructure has been received with widespread skepticism, not least in political circles and related to national security concerns. On the other hand, consumers have welcomed especially Huawei, whose sales of products continue to grow exponentially. In an African context, Chinese engagement has widely been welcomed, not least for the cheap provision of infrastructure technology and of smartphones. The difference between these contexts is not least the degree of involvement from ZTE, which enjoys a much larger presence in Africa than elsewhere, where it provides borderline totalitarian governments with telecom systems that may be used as tools of surveillance and potentially oppression, as we see it inter alia in Ethiopia.

While ZTE's strong bonds to the Chinese state remain undisputable, it is more difficult to determine the degree of influence of the Chinese state on Huawei. Especially in the Western context, it seems that the commercial potential of Huawei makes it questionable whether it would dare to engage in any substantial forms of industrial or political espionage. Thus far, scrutiny of Huawei has yet to expose any such activities, and actual exposure of espionage would seriously hamper, if not completely put an end to, Huawei involvement in telecom infrastructure in Europe, and eliminate its chances of ever being allowed to bid for US government contracts.

From a narrow national-security perspective, Huawei does not appear, thus, to represent any significant threat, not least because of the devastating effect that the exposure of e.g. espionage would have on its commercial activities. In that sense, we see a noteworthy difference between Huawei and ZTE, with the last appearing to represent a potentially greater security risk. In a wider sense, examination of Huawei's work in the UK and elsewhere have revealed that there might be issues with potential loopholes for hackers to exploit, unrelated to China and contingent on the technology used by the company, posing a more general cyber security risk. Furthermore, the decision to bypass other Scandinavian companies in contract tenders amounting to upwards \$1 billion (such as in the case of Denmark) naturally puts into focus economic security and the financial consequences of seeing funds in such sizes transferred out of the region.

The dilemma, especially in Denmark and elsewhere in Europe, remains that no other company, including Ericsson, Nokia Siemens Network or Orange, can provide advanced technology at the competitive prices that Huawei can. Whether the competitive prices can be attributed to favorable (and anti-competitive) agreements between Huawei and the Chinese National Development Bank (CDB) or similar financial institutions in China, as is widely claimed, is in principle unrelated. The issue, if one at all, can be seen to be that short-term financial concerns trump broader national interests, whether in regards to security or economic growth in the Scandinavian region.

For Denmark, the rule-set 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 transfer of network control back from Romania (where it had been outsourced to) to Denmark in a Network Operation Center, 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, but also require de facto adherence, something put into question a year ago where the Danish Broadcasting Corporation (DR) found that at least 35 Huawei employees worked in the NOC without proper security clearance.



China is actively seeking to expand its overseas investment in critical infrastructure, including in nuclear power and telecommunications. The major actors are big state-owned or big private companies, both of which receive strong state economic and diplomatic support. Economic motivations are important behind these initiatives, and China is an important investor due to economic slowdown in traditional developed economies. Infrastructure projects are nonetheless often expensive and can cause economic security problems or reliance of the host country on China, even though this has not been the focus of this report.

Because critical infrastructure has immediate connection with sovereignty and national security, Chinese involvement in this kind of sectors stirs up security concerns, in particular in Western countries. For information security, reviews 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 the indirect influence that the Chinese government could have on the companies, and that there exist loopholes in Chinese technology, which could be abused by hackers. How Chinese technology is used by host country governments is a concern as well, as it impinges on privacy and democracy.

For nuclear security and safety, Western-designed nuclear plants with Chinese financing and construction are expected to increase, their safety monitored by IAEA. The safety of China-built nuclear plants in Pakistan that use Chinese technology remains to be tested in the coming years. The risk of nuclear proliferation depends on whether recipient countries like Pakistan, Saudi Arabia and Iran abide by international rules.

Used as a foreign policy tool, investment in critical infrastructure enables China to obtain oil and gas resources and to enhance relations with a range of targeted host countries. China regards the agreement on projects as a measure of trust between the two countries, often rightly so. Countries that suspect China of using such investment for gaining access to crucial information and control over crucial assets for strategic purposes have rejected Chinese investment, even though they have not found or published solid evidence of such risks. Countries that seek to improve relations with China and focus on pragmatic economic gains would welcome Chinese investment, in a hope that their actions would gesture how much they value their relationship with China, though some put into place more stringent

monitoring mechanisms than others. In this sense, a country's perspective towards critical infrastructure and to what extent foreign involvement contains security risks varies depending on the political and economic environment in each country and can be subject to change over time.

## **Policy recommendations**

Based on the report's findings, it is recommended that:

- Host country governments should conduct their own assessment of security implications of Chinese and other foreign countries' involvement in the construction, operation and services in critical infrastructure, while avoid violating laws and conducting espionage. The security risks of allowing in companies from Western countries should not be overlooked either.
- A comprehensive approach to security-risk assessment of potential Chinese and other foreign companies' investments in critical infrastructure should be adopted. Security-related risks do not only involve short or medium-term national security, but extend to, for example, long-term economic security for both host country and investor country, political risks in third countries where Denmark is a joint investor, and regional and global security.
- Policymakers, the media and the public can learn from the information and investigations in other countries. Biases and presumptions about the close linkage between Chinese companies and the Chinese government should be avoided. It is also ill-advised to treat all Chinese companies the same way because they are as diverse as Western ones in their degree of globalisation and in their linkage to the government.
- Host country governments should set up adequate security measures to ensure information security in allowing foreign investments, including Chinese investment, in telecommunications. For instance, the host country government, in collaboration with regional or international organisations, can work with Chinese companies to ensure high technology and safety standards (including encryption, equipment and security clearances etc.) in order to avoid backdoors and weaknesses that are vulnerable to information leakage or malicious attacks.

- During the current process of nuclear technology upgrading, including in Chinese companies, international organisations including the IAEA can take the opportunity to set up renewed global security and safety standards. These include extraction and trade of raw materials, economic and environmental feasibility studies, construction and operation of nuclear power stations, emergency response, and transfer of nuclear technology. Countries with rich experience in nuclear technology, including France, Germany, Japan, Russia and the US, can contribute to this process.
- Security and safety measures agreed upon between the host country and Chinese companies have to be implemented and compliance should be regularly monitored by adequate mechanisms and should not be bypassed for contingencies or for speeding up commercial processes.
- In almost all the country-contexts studied, the public outcry and criticism concerning Chinese deals in telecommunications have been significant. These are likely to continue, yet may be appeased by increasing the transparency of commercial deals. Transparency remains by far the most efficient tool to demystify Chinese commercial engagement, and remains the responsibility of all engaged parts, from the Chinese investor to the Danish client and the Danish Ministry of Defence.

#### **NOTES**

- 1 IAEA country statistics: https://www.iaea.org/PRIS/CountryStatistics/CountryDetails. aspx?current=CN
- 2 'Westinghouse Electric's Chinese 'Trojan Horse", Forbes, 17 May 2016.
- 3 https://next.ft.com/content/62e7573c-2395-11e5-9c4e-a775d2b173ca
- 4 http://ip.reuters.com/article/china-uranium-idJPKCN0WG07Y
- 5 http://www.scmp.com/news/china/policies-politics/article/1906287/china-admits-nuclearemergency-response-inadequate. The white paper is available in Chinese here: http://www.scio.gov. cn/zxbd/wz/Document/1466424/1466424.htm
- 6 Russia is currently leading in exporting nuclear plants, with seven operating, four under construction, 14 contracted and 15 ordered. Russia is a world leader in fast neutron reactor technology, and exports of nuclear goods and services are also a major Russian policy and economic objective. http://www.world-nuclear.org/information-library/country-profiles/countries-o-s/russia-nuclear-power.aspx
  Thanks to the anonymous reviewer for pointing out this.
- 7 http://mainichi.jp/articles/20151230/ddm/008/030/080000c
- 8 World Nuclear Association, 'Nuclear Power in China', 25 May 2016.
- 9 Jost Wübbeke and Guan Ting, 'China's Nuclear Industry Goes Global', The Diplomat, 11 Feb. 2016.
- 10 Xinhua, 'China plans 30 overseas nuclear power units by 2030', 1 March 2016, http://en.people.cn/business/n3/2016/0301/c90778-9023576.html.
- 11 https://en.wikipedia.org/wiki/Ren\_Zhengfei
- 12 Intelligence and Security Committee (2013), Foreign involvement in the Critical National Infrastructure: The implications for national security. p.5
- 13 To the benefit of Greenland, p.10.
- 14 To the benefit of Greenland, p.9.
- 15 To the benefit of Greenland, p.11.
- 16 To the benefit of Greenland, p.15.
- 17 Boersma, Tim and Kevin Foley (2014), The Greenland Gold Rush: Promise and Pitfalls of Greenland's Energy and Mineral Resources, Brookings. P.2.
- 18 http://www.loc.gov/law/foreign-news/article/denmark-greenland-greenland-votes-to-lift-uranium-mining-ban-considers-independence/
- 19 http://www.theaustralian.com.au/business/mining-energy/greenland-minerals-poised-to-move-on-kvanefjeld-rare-earths-plan/story-e6frg9df-1225917279706
- 20 The Committee for Greenlandic Mineral Resources to the Benefit of Society (2014), To the benefit of Greenland, p.15.
- 21 Boersma, Tim and Kevin Foley (2014), The Greenland Gold Rush: Promise and Pitfalls of Greenland's Energy and Mineral Resources, Brookings. P.52.
- 22 http://www.world-nuclear-news.org/UF-Denmark-and-Greenland-reach-uranium-export-agreement-2001165.html
- 23 http://www.diis.dk/en/research/danish-greenlandic-declaration-towards-uranium-trade
- $24 \quad http://www.ggg.gl/docs/ASX-announcements/Denmark-Passes-Export-Legislation.pdf \\$
- 25 http://www.proactiveinvestors.com.au/companies/news/71183/greenland-minerals-and-energy-ltd-agrees-to-landmark-strategic-investment-71183.html
- $26 \quad http://markets.ft.com/data/equities/tearsheet/profile?s=600392:SHH$
- 27 https://next.ft.com/content/5136953a-1b3d-11e5-8201-cbdb03d71480
- 28 Burghart, Nora and Vanessa Rossi (2009), China's Overseas Direct Investment in the UK, Chatham House.
- 29 https://next.ft.com/content/e3125454-5402-11e6-9664-e0bdc13c3bef

- 30 The Economist, July 23 2016, p.10 "Britain's 'industrial strategy': Open for business?"
- 31 http://www.bbc.com/news/uk-politics-11564152
- 32 http://www.bbc.com/news/uk-england-somerset-20499033
- 33 https://www.edfenergy.com/energy/nuclear-new-build-projects/hinkley-point-c
- 34 http://www.areva.com/EN/news-9986/structure-of-the-partnership-for-hinkley-point-c-project.html
- 35 https://www.theguardian.com/environment/2013/oct/20/nuclear-power-station-hinkley-edf
- 36 http://mainichi.jp/articles/20151230/ddm/008/030/080000c
- 37 http://www.world-nuclear-news.org/NP-UK-confident-of-Hinkley-deal-18051601.html
- 38 https://next.ft.com/content/fc187680-774a-11e5-a95a-27d368e1ddf7
- 38 http://www.itv.com/news/westcountry/story/2015-10-21/hinkleys-construction-to-begin-within-weeks/
- 40 http://www.rist.or.jp/atomica/data/dat\_detail.php?Title\_No=14-02-03-07
- 41 https://www.theguardian.com/commentisfree/2015/oct/21/nuclear-power-deal-china-uk
- 42 https://next.ft.com/content/fcd6a462-7578-11e5-a95a-27d368e1ddf7
- 43 https://www.theguardian.com/business/2016/jun/17/edf-senior-managers-hinkley-point-postpone-letter-mps-energy-committee
- 44 Adding to the uncertainty is the challenge by Austria. It is reported that Austria is preparing to go to the European Court of Justice with an argument that the UK is breaching state aid rules by guaranteeing a set price for electricity produced at the reactor for 35 years. (https://next.ft.com/content/905342fa-b214-11e4-80af-00144feab7de#axzz4DoB0Kq8u)
- 45 https://www.theguardian.com/business/2016/may/13/hinkley-point-cgn-china-general-nuclear-power-corporation-edf-energy
- 46 https://next.ft.com/content/181077e2-54dc-11e6-befd-2fc0c26b3c60
- 47 It was reported that May had long been skeptical of the "gung-ho" approach that the UK government took, mainly by then-chancellor George Osborne, in making deals with Beijing. (https://www.theguardian.com/uk-news/2016/aug/01/osborne-rejected-safeguards-over-chinese-role-in-hinkley-point-says-ex-energy-minister)
- 48 https://www.theguardian.com/uk-news/2016/jul/29/hinkley-point-c-why-has-government-delayed-final-approval
- 49 Xiaoming Liu, 'Hinkley Point is a test of mutual trust between UK and China', Financial Times 8 August 2016
- 50 'Hinkley go-ahead after 'national security' safeguards', Financial Times, 15 Sep. 2016.
- 51 NSG is a group of major nuclear supplier countries, including Denmark, that seek to prevent nuclear proliferation by controlling the exports. NSG prohibits the supply of nuclear equipment to non-signatories of the NPT.
- 52 'China's 'unusual' nuclear pact with Ukraine's Yanukovich', 7 March 2014 http://america.aljazeera.com/articles/2014/3/7/china-s-unusual-nuclearpactwithukrainesyanukovich. html. The Agreement to Further Deepen Strategic Partnership between China and Ukraine can be found (in Chinese) at:
- 53 http://news.xinhuanet.com/politics/2013-12/05/c\_118439894.htm.
- http://mfa.gov.ua/en/press-center/news/45831-kitajsyki-atomniki-zacikavleni-u-spivrobitnictvi-z-ukrajinoju-v-jadernij-galuzi
- 54 http://www.huawei.com/en/news/2016/1/Huawei-and-TDC-Group
- 55 http://www.tek.no/artikler/venstre-deler-amerikanernes-frykt-for-huawei/113450
- 56 http://telecoms.com/17374/ericsson-stalls-huaweis-move-into-sweden/

- 57 http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=4543334
- 58 'Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE', US House of Representatives 112th Congress, 8 October 2012, https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20 report%20(final).pdf.
- 59 Dan Steinbock, 'Huawei in America: An NSA Retrospective', China-US Focus, 1 April 2014, http://www.chinausfocus.com/finance-economy/huawei-in-america-an-nsa-retrospective/.
- 60 'White House-ordered review found no evidence of Huawei spying: sources', Reuters, 18 October 2012, http://www.reuters.com/article/us-huawei-spying-idUSBRE89G1Q920121018.
- 61 Eric Harwit, 'Sanctioning ZTE and Huawei: Chinese Telecom Giants' Conflicts with the U.S.', China-US Focus, 30 June 2016, http://www.chinausfocus.com/finance-economy/sanctioning-zte-and-huawei-chinese-telecom-giants-conflicts-with-the-u-s/.
- 62 'N.S.A. Breached Chinese Servers Seen as Security Threat', The New York Times, 22 March 2014.
- 63 UKTI, Investments from China.
- 64 http://huawei.com/uk/about-huawei/huawei-uk/index.htm
- 65 Intelligence and Security Committee (2013), Foreign involvement in the Critical National Infrastructure: The implications for national security, p.23.
- 66 http://pr.huawei.com/en/news/hw-093468-ukcenter-security.htm#.V4-PhmPGfUB
- 67 Intelligence and Security Committee (2013), Foreign involvement in the Critical National Infrastructure: The implications for national security, p.15.
- 68 https://www.gov.uk/government/uploads/system/uploads/attachment\_data/file/205680/ISC-Report-Foreign-Investment-in-the-Critical-National-Infrastructure.pdf
- 69 http://www.bbc.com/news/world-asia-china-34539507
- 70 http://www.huawei.com/en/news/2016/5/Huawei-and-UKTI-sign-MoU
- 71 http://www.reuters.com/article/britain-eu-javid-huawei-tech-idUSU8N19701M
- 72 https://next.ft.com/content/73fbae2c-f81c-11e5-96db-fc683b5e52db
- 73 https://www.gov.uk/government/uploads/system/uploads/attachment\_data/file/525410/ncsc\_prospectus\_final\_version\_1\_0.pdf

### **Photos**

Coverphoto: iStock photo, Marilyn Haddrill

Page 4-5: Scanpix Denmark, Xinhua

Page 12-13: Scanpix Denmark, MARTIN BOND/SCIENCE PHOTO LIBRARY

Page 28-29: Scanpix Denmark, GAETAN BALLY

Page 44-45: iStock photo, RapidEye

## DIIS · Danish Institute for International Studies

The Danish Institute for International Studies is a leading public institute for independent research and analysis of international affairs. We conduct and communicate multidisciplinary research on globalisation, security, development and foreign policy. DIIS aims to use our research results to influence the agenda in research, policy and public debate, and we put great effort into informing policymakers and the public of our results and their possible applications.

## **Defence and Security Studies at DIIS**

This publication is part of the Defence and Security Studies that DIIS carries out for the Danish Ministry of Defence. The aim of these studies is to provide multidisciplinary in-depth knowledge on topics that are central for Danish defence and security policy, both currently and in the long term. The design and the conclusions of the research are entirely independent. Conclusions do not reflect the views of the ministries involved or any other government agency, nor do they constitute an official DIIS position. Additional information about DIIS and our Defence and Security Studies can be found at www.diis.dk.

