China, Information Technology, and the Arab World

https://www.e-ir.info/2011/04/24/china-information-technology-and-the-arab-world/

WILLIAM A. FOSTER AND HANNAH THORESON, APR 24 2011

The Chinese government has developed the world's most extensive technical, organizational, and cultural systems for monitoring and filtering the Internet and other forms of communications such as SMS (short messaging service) and voice calls. In 1996, the Chinese State Council decided to embrace the Internet as a key towards opening China up to the world, but decided to set things up so that the Chinese government could remain in control of communications. In my PhD dissertation that was published by CISAC at Stanford University on*The Diffusion of the Internet in China* [1] , I traced the evolution of China's Interconnecting network regime. China decided that it could not have just any organization (government agencies, state owned enterprises, private businesses, Western telecom companies) offer Internet connections to the outside world. At the same time, it was not politically possible to have only one government body providing a monopoly service. Therefore, the Informatization Group of the State Council chose to allow nine government bodies to run Interconnecting networks to the outside world. Under this state controlled competition, the interconnecting networks competed with each other to increase services and lower price while taking responsibility for ensuring that its users did not use the Internet in any way that threatened the state.

Each interconnecting network put up a gateway that blocked traffic of Internet sites that were deemed as dangerous such as sites of news organizations (like the New York Times, etc.), social networking sites (Facebook and Wikipedia for example), and the sites relating to Taiwanese independence or those of Dalai Lama, the Tibetan spiritual leader. Thousands of sites were censored. With state bodies using deep packet inspection methods, the URLs of individual pages were filtered for key phrases. And recently, sites mentioning the political unrest in the Arab world have also been blocked.

Each interconnecting network was responsible for blocking a different set of sites. For example, the Chinese Academy of Science's network, whose users were more trusted, blocked fewer sites than the interconnecting network run by China Telecom, which catered to the general public. CERNET, the university network which supervised a population that the State Council considered both dangerous and the key to China's progress, put in place a system where each foreign site that a student visited was tracked in the name of charging the student for access. Over time more and more regulations were put in place to ensure that Internet Cafés, internet service providers, and chat rooms took responsibility for the actions of their customers and became tools of the Ministry of Public Security. By 2001, the Ministry of Public Security also had 30,000 Internet police forces who monitored Internet use in China. Currently, Freedom House estimates that there are over 100,000 people in China involved in policing the Internet [ii] Over the past 15 years the monitoring capabilities of the Chinese government both at the interconnecting network gateway as well as throughout the network have become more sophisticated. US and European telecommunications companies developed and sold some of their most advanced technologies to the People's Republic of China (PRC). At the same time, a thriving security and telecommunications industry began to develop in China.

The Chinese Telecom Manufacturers Huawei and ZTE got their start manufacturing equipment for China's provinces and really got going in 1998-2000 when China's Ministry of Information Industries (MII) had the four commercial interconnecting networks roll out state-of-the-art national VoIP (Voice over IP) networks. Huawei and ZTE soon found a ready market for their telecommunications equipment in Africa, the Middle East and the rest of Asia. Because a research and development (R & D) engineer costs Huawei or ZTE less than one fifth of what it would cost a telecom company in the West, these two companies were able to offer a great deal of customization to meet the special

needs of a telecom company including integrating legacy systems with next generation network technology.

Many Arab countries have bought telecommunications equipment from the telecom manufacturing giants Huawei and ZTE and have tried to emulate the Chinese monitoring and filtering regime. Table 1 below shows the wide range of telecommunications equipment that Huawei and ZTE are selling to the Arab world. Having originally sold standard GSM (Global System for Mobile Communications) technology to the Arab states of the Middle East and North Africa, these two companies are now selling fourth generation (4G) networks based on WiMax technologies. They are building state of the art fiber-based data networks with FTTH (Fiber to the Home).

Table 1: China's Presence in the Arab world

The post-soviet states of Central Asia	Share of agricultural labour force in total labour force[2]	The Economist Intelligence Unit's index of democracy[3]
Turkmenistan	31.1%	1.72
Tajikistan	29.9%	2.51
Uzbekistan	23.8%	1.74
Kyrgyz Republic	22.8%	4.31
Kazakhstan	15.2%	3.3

The post-soviet states of Caucasus	Share of agricultural labour force in total labour force [2]	The Economist intelligence Unit's index of democracy [3]
Azerbaijan	24,4%	3,15
Georgia	16,9%	4,59
Armenia	10,6%	4,09

Based on their global success, Huawei has grown to a US$ 28 billion company (2010) and ZTE into one worth US$ 10.7. While ZTE is a publicly traded company on the Hong Kong stock exchange, Huawei is a private employee owned company which just recently announced its board of directors. Before founding Huawei, the company's

President, Ren Zhengfei, worked for the People's Liberation Army. He has cultivated personal relationships (guanxi) with a broad section of China's leadership. The US Senator John Kyl (R-AZ) and a number of his colleagues have tried to ban Huawei from supplying infrastructure to the United States out of fear of the ties between Huawei and the Chinese government. There is a fear that Huawei or ZTE might perpetrate espionage against US targets by inserting "Trojans" into their equipment. There has also been similar concern in India, but the Arab world does not seem to share these reservations. Taking advantage of security tools and techniques developed in the Chinese market, Huawei and ZTE help their overseas partner telecom companies fashion networks that meet the information control needs of their domestic governments. It is well known that most of the states listed in Table 1 monitor their national telecommunications networks.

During the recent revolution in Egypt, Internet access was shut off nationwide for five days and text messaging was frequently unavailable as well. The global technology community reacted to Mubarak's success in cutting his nation off from the world with shock, but a clear analysis of Egypt's telecommunications infrastructure reveals that the network was likely designed with that purpose in mind. The physical cables, towers, and transmitters were mostly designed and built by Huawei, but were owned by the Egyptian government. Chinese and Egyptian IT ministries signed a memorandum of understanding when the initial investment deal was brokered in 2002 and Huawei has continued to work closely with local government authorities in Egypt as it keeps expanding and hires workers from the area [iii]. Iran's telecommunications infrastructure was also largely built via contracts with Chinese firms. After street protests over June 2009 presidential election results, the Iranian government has been developing one of the most sophisticated online surveillance systems in the world. It has been reported that Iran is employing foreign experts, but does not report their nationality [iv]. Finally, Huawei built the cell phone network for Libya. The cell phone network was designed to top route all traffic through Tripoli, the capital, so that the central government would be able to monitor and control all traffic. At the beginning of the Libyan popular rebellion, the rebels were not able to use their cell phones as Huawei refused to provide the rebels with switches to connect their cell phones [v]. This would seem to indicate a preference for working with established government authorities – whomever they may be – rather than simply selling to anyone with the money to buy.

—

Dr. William Abbott Foster *is a faculty associate at Arizona State University Polytechnic. His academic research centers broadly on the relationship between technology, society and politics. He can be contacted via email at WAFoster@asu.edu.*

Hannah Thoreson *is an undergraduate at Arizona State University, and can be reached via email at hthoreso@asu.edu.*

Notes

[i] The dissertation is available at www.FosterandBrahm.com/docs/chinainternet.pdf.

[ii] Freedom House, "Freedom on the Net 2011", Available at http://www.FreedomHouse.org/template.cfm?page=664, Accessed April 18, 2011.

[iii] Arab Republic of Egypt, "Egypt and China sign a MOU For the development of the CIT Industry," available at http://mcit.gov.eg/MediaPressSer_Details.aspx?ID=989@TypeID=1, Accessed on April 21, 2011.

[iv] Neal Ungerleider, "Iran Cracking Down Online with Halal Internet," *Fast Company*, April 18, 2011. Available at http://www.fastcompany.com/1748123/iran-launching-halal-internet Accessed April 19, 2011.

[v] Margaret Coker and Charles Levinson, "Rebel's Hijack Gadhafi's Phone Network," *Wall Street Journal*, April 13, 2011. Available at http://online.wsj.com/article/SB10001424052748703841904576256512991215284.html Accessed April 19, 2011.