merics
Mercator Institute
for China Studies

China Monitor
Issue 22 | 21 April 2015
Revised Version 22 April 2015

Cyber Security in China: Internet Security, Protectionism and Competitiveness: New Challenges to Western Businesses

Cyber sovereignty, intensified internet censorship, shadow IT economy.

by Hauke Johannes Gierow

MAIN FINDINGS AND CONCLUSIONS

- China is resolutely moving forward with development of its own IT industry. It is also isolating itself from international IT technology. By exercising control over major state-run businesses, the PRC is also maintaining its sovereign position in the IT sector.

- The government supports the international expansion and sales endeavours of Chinese IT companies – the 'national champions'. This blend of political and economic factors frequently gives rise to security questions among customers from Western countries.

- China is developing parallel standards in the software and hardware sectors. In addition, alternative encryption standards, operating systems and competing app stores are earmarked for enhancing China's independence in the IT sector. However, inadequate quality regulations are posing a threat to IT security.

- Censorship and restrictions on internet connections place constraints on China as a business location. Concerns about IT espionage and theft of company secrets driving international businesses to transfer personnel or entire departments to other Asian countries.

- Chinese internet users are threatened by a shadow IT economy. Illegal programs are often installed on computers and are not provided with security updates. Hackers can gain access to these unprotected computers and use them as a base for worldwide attacks.

- Instead of insistently calling for fundamental changes in Chinese internet policy, the Federal Government of Germany ought to negotiate specific improvements for German businesses, for example in terms of market access or protection of intellectual property rights.

1 No internet security without independent technology

At the beginning of 2014, an alliance of fifteen private Chinese IT manufacturers was founded in the Beijing district of Zhongguancun (中关村), the Chinese equivalent of Silicon Valley. They stepped up endeavours to develop a Chinese operating system based on Linux that would run on government computers and the computers of security relevant businesses such as banks. **By taking this step, Beijing hopes to gain protection from espionage from the USA and demonstrate the innovative power of the Chinese IT economy.**[1]

In spite of the rampant growth of its IT industry, China is still dependent upon foreign technology at the moment. According to Xinhua, the state news agency, ninety per cent of its microchips and sixty-five per cent of its firewall products originated in other countries in 2012, primarily the US.[2] The government views foreign technology as a potential threat to national security. Covertly installed back doors enable surveillance of computers and networks, for example. Therefore, stringent constraints on the use of foreign IT products are already in place in areas critical to security.

At the same time, sealing the domestic market off from external influence is intended to foster the development of industrial and innovation policies in China: the government in Beijing wants to strengthen the competitiveness of domestic IT companies[3] (see issue 20 of MERICS China Monitor).

2 Cyber security: opportunities and costs for the Chinese IT economy

2.1 Targeted promotion by the state

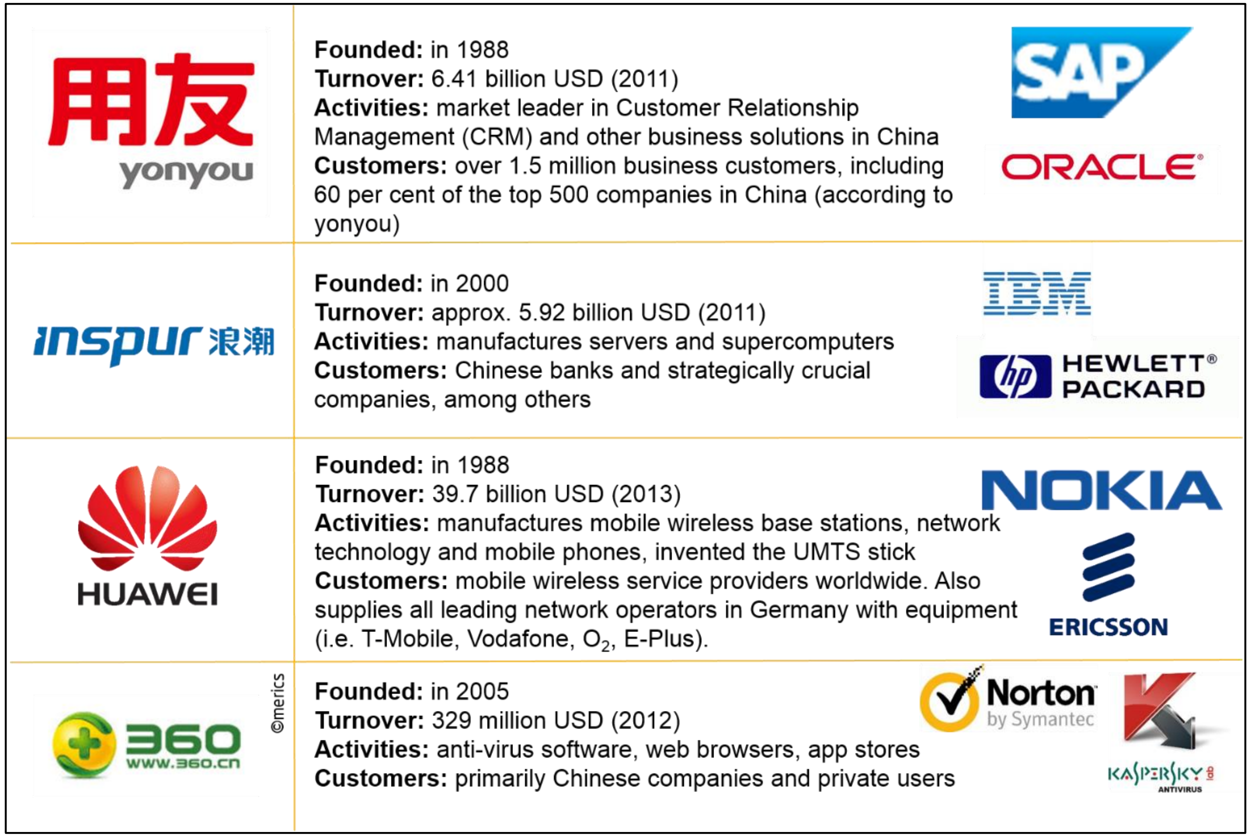
The Chinese government has succeeded in promoting a dynamic IT industry with robust private companies while retaining control over the sector. State-run telecommunications companies (China Telecom, China Unicom and China Mobile) dominate the market with their investments. Decisions they make, usually approved by the government, determine what kind of technologies will be developed, thus defining the framework conditions for the industry and its regulation.[4] In addition, the government promotes its own technological standards through state-run programs, generally in close collaboration with Chinese IT companies such as ZTE, Lenovo and Datang Mobile.

Chinese companies are becoming increasingly successful in the field of IT infrastructure, a fact that is partly due to state support. In addition to Huawei and ZTE, both network equipment suppliers of international repute, new companies are also gaining a foothold in the market now: businesses such as Inspur and Dawning Industries (曙光) are using Chinese technology to develop servers and supercomputers for complex computing tasks, up to now mostly for the domestic market (see Figure 1). **This technology is particularly relevant to secure networks since even small mistakes in the programming code can destroy the basis for secure IT products.**

China will become more independent of foreign IT products in the years to come. However, there is no consensus among experts on whether this independence will enhance network security on the whole. Meeting quality standards, for instance by monitoring the supply chain or having an independent examination of the source code, is a crucial criterion for software security. Many IT companies in China ignore these standards, though.

Encryption technologies are a different problem: This part of the IT infrastructure not only protects hard drives and documents, but it also shields internet connections from unauthorised access. However, the strict import regulations imposed on Chinese companies only allow them to adopt international encryption standards such as RSA, which is used by many governments and corporations, in exceptional cases. Instead, they must rely on Chinese encryption methods, which only provide partial protection. Chinese suppliers have to deposit a type of ‘skeleton key’ with the National Encryption Leading Group (国家密码管理局) (referred to as the Key Escrow procedure).[5] This procedure protects data from hackers and foreign governments, but the government in Beijing can gain access to it at any time via the skeleton key.

Figure 1: Chinese IT suppliers and their Western competitors (by the author, Hauke Gierow)



用友 yonyou	**Founded:** in 1988 **Turnover:** 6.41 billion USD (2011) **Activities:** market leader in Customer Relationship Management (CRM) and other business solutions in China **Customers:** over 1.5 million business customers, including 60 per cent of the top 500 companies in China (according to yonyou)	SAP ORACLE
inspur 浪潮	**Founded:** in 2000 **Turnover:** approx. 5.92 billion USD (2011) **Activities:** manufactures servers and supercomputers **Customers:** Chinese banks and strategically crucial companies, among others	IBM hp HEWLETT PACKARD
HUAWEI	**Founded:** in 1988 **Turnover:** 39.7 billion USD (2013) **Activities:** manufactures mobile wireless base stations, network technology and mobile phones, invented the UMTS stick **Customers:** mobile wireless service providers worldwide. Also supplies all leading network operators in Germany with equipment (i.e. T-Mobile, Vodafone, O_2, E-Plus).	NOKIA ERICSSON
360 www.360.cn ©merics	**Founded:** in 2005 **Turnover:** 329 million USD (2012) **Activities:** anti-virus software, web browsers, app stores **Customers:** primarily Chinese companies and private users	Norton by Symantec KASPERSKY ANTIVIRUS

2.2 Going out – both an opportunity and challenge for Chinese companies

With their products, Chinese IT firms are stepping up competition with Western companies in developing and emerging countries.

The Chinese Ministry for Industry and Informatisation（中华人民共和国工业和信息化部）has pursued the *‘Going Out’* strategy（走出去）ever since 1999. This is used to support successful Chinese companies and make them internationally competitive. It has been expanded to include the IT sector as well. Low-interest loans and the active support of Chinese embassies are the tools with which the government intends to enhance the competitiveness of these national champions on international markets.[6] Huawei, for example, was granted a low-interest loan of ten billion USD by the China Development Bank to finance its international expansion.[7]

But this systematic promotion of the IT sector also presents problems for Chinese companies: technology from the PRC is perceived as a threat to security by other countries, even though there has been no concrete evidence that the government has placed any back doors in routers, mobile phones or other devices to date. Huawei offered to equip the London Underground with mobile wireless technology for the 2012 Olympic Games free of charge, an offer worth more than 500 million CNY (approx. 65 million EUR), but the British side rejected the offer for security reasons.[8]

Both businesses and the Chinese government are now trying to stem the loss of confidence in their products. Huawei, for example, has launched a transparency drive to deal with concerns in Europe. The company has established a research centre in the UK to enable independent security audits of their program code by the British government.[9]

The world’s third-largest mobile phone manufacturer, Xiaomi (小米), is employing a different tactic: to eliminate concerns about back doors in their own cloud services in China, the company is setting up ‘local clouds’ in key markets such as India. Local users can deposit their contacts, calendar entries and other data there instead of in China. This measure is probably intended to build up user confidence in the brand more than anything else, however.

In spite of initial misgivings, Chinese companies are already enjoying great success in some foreign markets. Huawei and Lenovo now rank among the leading manufacturers of IT products for the European and American consumer market, for example. Lenovo actually overtook Hewlett-Packard, the previous market leader in the PC sector, in 2014 by securing a market share of almost seventeen per cent.[10]

Chinese IT companies even keep pace with global leaders in the area of mobile-communications infrastructure. While the Chinese alternative to UMTS, TD-SCMA, is only used in Nicaragua and Zimbabwe outside China, networks with the new Chinese FDD-LTE are part of network infrastructure in Germany and other European countries.

2.3 Alternative ecosystems: their own app stores and operating systems, but with security gaps

Users in China are situated in a unique digital ecosystem. Chinese alternatives have been developed for many applications from the West.

In Germany, users of Android devices download apps or digital content such as films and books primarily through Google’s own app store, *Google Play.* However, *Google Play* is blocked in China, and companies such as Baidu, Tencent or Qihoo 360 offer alternative app stores. Compared to *Google Play,* however, they have severe security drawbacks. A review of 7,000 apps infested with viruses revealed that 95 per cent of them were offered in Chinese app stores.[11] A mobile-phone virus developed by a student infected over 100,000 Android devices in China within only a few hours. The virus spread via the user’s address book and enabled control over almost all of the device’s telephone functions.[12]

The Chinese government also plans to distribute alternative systems on the PC market. For more than five years, it has therefore been pushing the development of its own operating systems hard. From 2015 onwards, fifteen per cent of all computers in every official office are to be converted from Windows to Chinese operating systems. The best-known systems are *NeoKylin OS* and *Red Flag Linux.* Chinese technologies have not reached full maturity yet, however: users complain about compatibility problems, lack of software alternatives and inadequate user-friendliness – a deficit expected to be eliminated by domestic IT companies forming an alliance, as mentioned earlier.

2.4 The high cost of internet censorship

Isolationism and protectionism lead to another problem for Chinese IT companies: the obligation to censor the internet. Not only does censorship affect freedom of speech, but it also impacts the entire economy.

Operating a social network in China is expensive. The State Council Internet Information Office (国家互联网信息办公室) places tight restrictions on information from the internet. To comply with these controls, ISPs are required to employ two to three censors per 50,000 users.[13] For Sina Weibo, with around 300 million users, this means employing 15,000 people for the sole purpose of monitoring the content of the web pages the users invoke – a huge undertaking with considerable financial repercussions. By comparison, the sector's leader, Facebook, employs a total of only 8,500 staff worldwide.[14]

Internet censorship also impairs the development of software and apps. Google and other ISPs grant developers global access to program libraries and web fonts free of charge. This service helps programmers save time and money. Since data in China is blocked by internet censorship, programmers there have to redevelop the data themselves.[15]

3 *Cyber security* – a key location factor for foreign companies

3.1 Censorship and cyber attacks hurt business

Foreign companies in China must comply with ever more stringent regulations in the IT sector, impeding their ability to protect business secrets and hindering international co-operation.

China represents the largest market in the world for Apple; the iPhone is very popular there. In October 2014 it became known that hackers had targeted data transmission to the company's iCloud service. Due to the complexity of the hack, IT experts suspect that the Chinese government was behind the attack or at least knew about it.[16] However, just a few days later, Apple's chief executive, Tim Cook, went to Beijing and held discussions with key decision-makers at party headquarters, Zhongnanhai (中南海). This shows that Beijing has to deal with security reservations on the part of large Western companies in spite of its market power.[17]

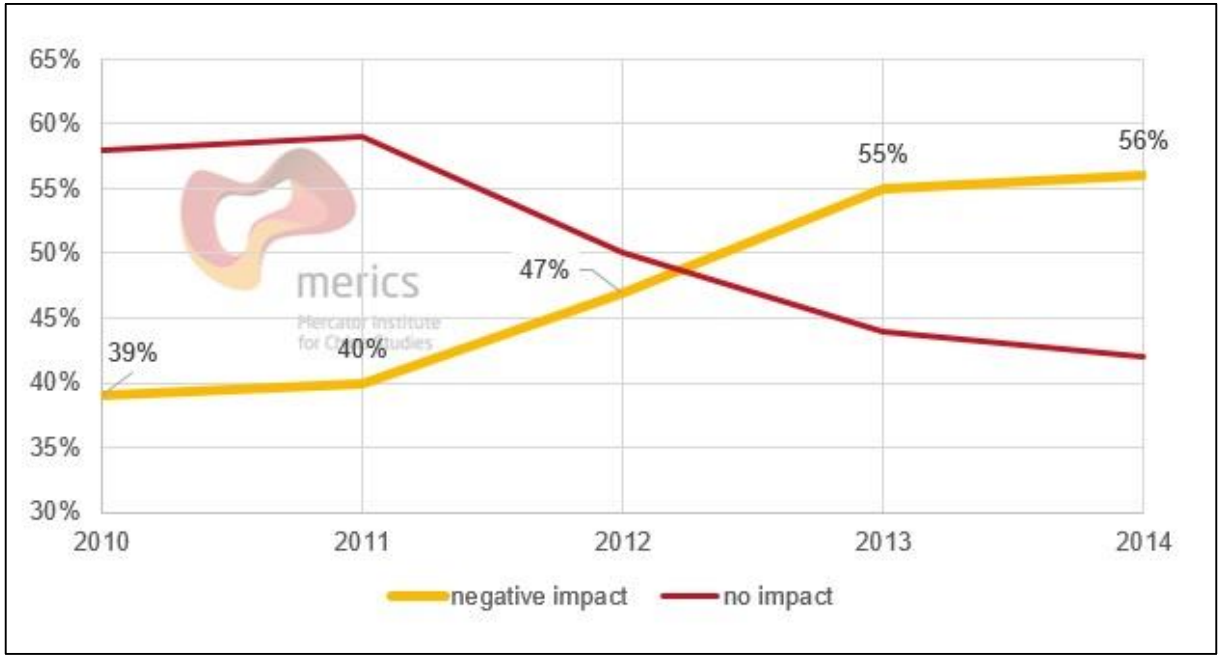
Other companies also feel the impact of cyber attacks and censorship. International collaboration with services such as Gmail, Google Docs or Dropbox is becoming increasingly dysfunctional. The same applies for virtual private networks (VPNs), with which users seek protection for information and business secrets. [18] Routine workflows of global corporations only function to a limited extent in the People's Republic of China. In international companies, for instance, many business applications such as statistics and database programs are not run on local computers, but rather on servers based at corporate headquarters. If connections are slow or VPNs unstable, these applications cannot always be accessed from China. Even simply transferring files to colleagues in other countries can be a trying experience.

More than half the American companies questioned in a recent survey by the American Chamber of Commerce in China indicated that internet censorship is detrimental to their business (see Figure 2).[19] Recently stepped-up blockades of websites and online tools have accelerated this tendency even further. Over eighty per cent of the European companies in China report of negative impact on their business prospects. Thirteen per cent have even postponed investments in R&D due to current events.[20]

The media report that international corporations such as General Motors are already in the process of moving their Asian headquarters to Singapore, Japan or Vietnam. Their reasons for doing so include not only censorship, but also factors such as poor air quality and inadequate protection of intellectual property.[21]

Many companies, including those in the digital sector, have been complaining about industrial espionage for years. Company secrets and construction plans are favourite targets of Chinese hackers.

Figure 2: Internet censorship and competitiveness (by the author, Hauke Gierow)



Question asked: How does censorship of content on the internet impact the ability of your company to conduct routine business in China? Source: AmCham China (2014): 15f.

American cyber-security companies and the FBI blame the Chinese government for supporting and even engaging hackers. Hard evidence of this is scarce, however, as professional hackers are capable of covering their tracks or leaving false trails.

3.2 Parallel technical standards are a challenge to Western companies

Western suppliers on the Chinese market have to conform to parallel Chinese IT standards. The Chinese wireless LAN technology called WAPI

(‘WLAN Authentication and Privacy Infrastructure’) is one example. Even though WPA2 encryption has become the international standard, China has deliberately gone separate ways since 2003. For foreign suppliers of routers and WLAN-compatible devices, this means they have to share their source code with one of eleven licensed Chinese IT companies and contribute to the development of the WAPI standard. Due to insufficient WAPI support, Apple was not allowed to sell the first version of its iPhone in China in 2010 until adjustments were made.[22]

Now, Apple will be the first Western IT company to have its products tested in China for compatibility with Chinese security standards. Lu Wei, head of the State Council Internet Information Office, made an announcement to this effect in January 2015. Thus, the company is presumably sharing confidential information with the government.[23] IT companies such as CISCO, Qualcomm and Microsoft will also have to make concessions if they want to enjoy continued access to the Chinese market in the future.[24]

4 Illegal IT shadow economy

4.1 Piracy poses a security problem

Disputes between Chinese and Western IT companies over their market share and market access are rather secondary to the security of users in China. For them, it is imperative that they are able to shop securely online and that their computers cannot be hacked.

There are major electronics markets in cities such as Shenzhen and Hong Kong. Visitors have a wide selection of software and hardware products to choose from, many of which are manufactured and distributed illegally, however.

Software piracy is clearly harmful to Western manufacturers: according to their own figures, they lose billions in licence fees. Former Microsoft head Steve Ballmer, for instance, once indicated that ninety per cent of the company’s products in China were being used illegally.[25] What’s more, pirated copies generally do not include any security updates, a fact that is especially problematical in key components such as operating systems. Susceptible devices are not only a security hazard for their users, they also threaten network security worldwide:[26] if security gaps are not closed up, criminals can gain access to users’ devices and employ these as ‘zombie computers’ in botnets. This enables them to steal additional access data from users or attack websites or network infrastructure. Illegally sold operating systems also frequently contain deliberately embedded viruses.

4.2 Hacker networks in China

Criminal hackers are a menace to the well-being and privacy of Chinese internet users. Illegal services are unabashedly offered in public forums, so there is obviously little fear of prosecution.

The ways and means with which illegal services are offered and advertised in China differ fundamentally from those in Western countries. While trade in stolen passwords or credit-card data generally runs via encrypted networks, Chinese hackers co-ordinate their illegal activities in open chat groups in QQ or forums run by Baidu. One reason for this is that Tor[27], an internet anonymizer service, is blocked in China.

A wide variety of often reasonably priced services is offered. Criminals can purchase access to servers with which they can infect users with malware or send spam messages. Custom-made Trojan horses or creation of counterfeit sign-in pages for banks and social networks are also available – thus, PCs and smartphones can also be spied on (see Figure 3).

5 German policy against Chinese protectionism

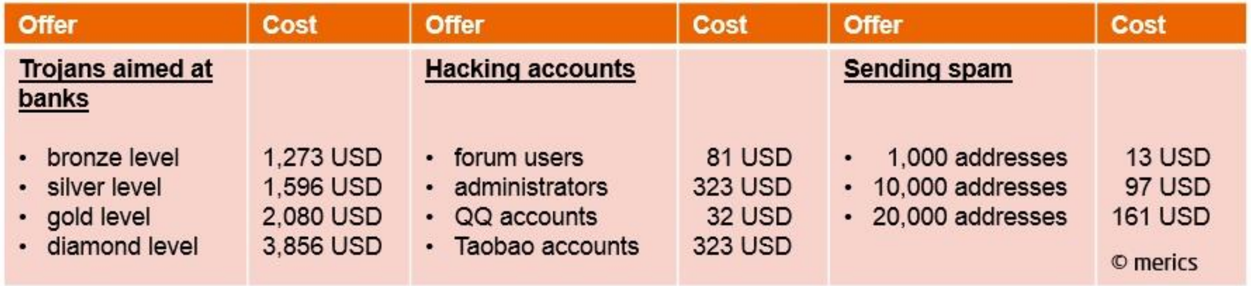
China's steady expansion of its own IT industry and growing isolation from foreign products have been felt keenly by international manufacturers. Germany's cyber policy towards China must be prepared for conflict. In the long run, China will not agree to become integrated into a cyber-security system defined by Western concepts. In fact, Beijing is already working with other newly industrialised countries on parallel standards for internet governance, which has been dominated by the West up to now.

As far as IT services and products for high-tech sectors are concerned – for instance in the area of Industry 4.0 and specialised business software – German companies can rely on their competitiveness in the face of Chinese rivals. The question is, for how much longer? It would therefore be wise for Germany to pursue a policy that has already proved to be effective in other fields.[28] Instead of working towards fundamental change in Chinese cyber security, the Federal Government of Germany should focus on pragmatic goals that are attainable in practice. After all, there are enough urgent topics to be dealt with as it is, such as better protection of intellectual property or secure market access for German companies.

Your contact for this issue of *China Monitor*:
Hauke Gierow
Hauke.Gierow@merics.de
Editor: Silke Ballweg

Publisher's details:
Mercator Institute for China Studies
Klosterstr. 64
D-10179 Berlin
phone: +49 30 3440 999-0
e-mail: info@merics.de
www.merics.org

Figure 3: Sample of 'services' offered by criminal hacker networks (by the author, Hauke Gierow)



Offer	Cost	Offer	Cost	Offer	Cost
Trojans aimed at banks		**Hacking accounts**		**Sending spam**	
• bronze level	1,273 USD	• forum users	81 USD	• 1,000 addresses	13 USD
• silver level	1,596 USD	• administrators	323 USD	• 10,000 addresses	97 USD
• gold level	2,080 USD	• QQ accounts	32 USD	• 20,000 addresses	161 USD
• diamond level	3,856 USD	• Taobao accounts	323 USD		© merics

Source: Trend Micro (2013).

[1] Zhang, Yu (2014). ‘Homegrown developers look to unseat Microsoft's dominant OS’, http://www.globaltimes.cn/content/887716.shtml. Accessed on 24 October 2014.

[2] Zhangwei 张卫 (2012). ‘信息安全的机遇与挑战’ (Opportunities and Challenges of Information Security). http://news.sohu.com/20120416/n340660958.shtml. Accessed on 15 September 2014.

[3] Zhonghua renmin gongheguo guowuyuan 中华人民共和国国务院 (2012). ‘国务院出台意见推进信息化发展切实保障信息安全’ (The State Council publishes a document on promoting the development of informatisation and for the protection of cyber security). http://politics.gmw.cn/2012-07/17/content_4571519.htm. Accessed on 14 August 2014.

[4] Ernst, Dieter and Naughton, Barry (2008). ‘China’s emerging industrial economy: insight from the IT industry’, in: McNally, Christopher A. (ed.) (2008). *China’s Emergent Political Economy – Capitalism in the dragon’s lair*, 39–59. London and New York: Routledge.

[5] Cloutier, Christopher T. and Cohen, Jane Y. (2011). ‘Casting a wide net: China’s encryption restrictions’, http://www.kslaw.com/imageserver/KSPublic/library/publication/2011articles/11-11WorldECRCloutierCohen.pdf. Accessed on 15 August 2014.

[6] Wang, Yukai 汪玉凯 (2014). ‘中央网络安全与信息化领导小组的由来及其影响’ (The origins and impact of the Central Cyber Security and Informatisation Leading Group). http://theory.people.com.cn/2014/0303/c40531-24510897.html. Accessed on 22 October 2014.

[7] Nolan, Peter (2014). *Chinese Firms, Global Firms: Industrial Policy in the Era of Globalisation*. New York: Routledge.

[8] Fauna (2011). ‘Huawei’s London Underground Bid Blocked, Chinese Reactions’, http://www.chinasmack.com/2011/stories/huaweis-london-underground-bid-blocked-chinese-reactions.html. Accessed on 30 November 2014.

[9] Kan, Michael (2013). ‘UK to probe Huawei's cybersecurity evaluation center’, http://www.pcworld.com/article/2044722/uk-to-probe-huaweis-cybersecurity-evaluation-center.html. Accessed on 22 October 2014.

[10] Gartner (2014). ‘Gartner Says Worldwide PC Shipments Declined 6.9 Percent in Fourth Quarter of 2013’, http://www.gartner.com/newsroom/id/2647517. Accessed on 22 September 2014.

[11] Eddy, Max (2013). ‘Nearly 7,000 Malicious Android Apps Infest China's Appstores’, http://securitywatch.pcmag.com/mobile-security/315218-nearly-7-000-malicious-android-apps-infest-china-s-appstores. Accessed on 22 September 2014.

[12] Muncaster, Phil (2014). ‘Chinese Heart App Virus Slams 100,000 Android Phones’, http://www.infosecurity-magazine.com/news/chinese-virus-100000-android-phones/. Accessed on 22 September 2014.

[13] King, Gary, Pan, Jennifer and Roberts, Margaret E. (2014). ‘Reverse-engineering censorship in China: Randomized experimentation and participant observation’, *Science* 345 (6199): 1–10.

[14] Facebook Newsroom (2014). Company Info. http://newsroom.fb.com/company-info/. Accessed on 30 November 2014.

[15] Bradsher, Keith and Mozur, Paul (2014). ‘China Clamps Down on Web, Pinching Companies Like Google’, http://www.nytimes.com/2014/09/22/business/international/china-clamps-down-on-web-pinching-companies-like-google.html?_r=0. Accessed on 25 September 2014.

[16] Franceschi-Bicchierai, Lorenzo (2014). ‘Apple Addresses iCloud Attacks While China Denies Hacking Allegations’, http://mashable.com/2014/10/21/apple-icloud-attacks-china/. Accessed on 22 October 2014.

[17] Lovejoy, Ben (2014). ‘Tim Cook meets with Chinese vice premier in Beijing following iCloud phishing attack’, http://www.techgreatest.com/apple-news/tim-cook-meets-with-chinese-vice-premier-in-beijing-following-icloud-phishing-attack/. Accessed on 3 December 2014.

[18] Arthur, Charles (2011). ‘China cracks down on VPN use’, http://www.theguardian.com/technology/2011/may/13/china-cracks-down-on-vpn-use. Accessed on 3 December 2014.

[19] American Chamber of Commerce in China (2013). ‘Business Climate Survey 2013’, http://web.resource.amchamchina.org/cmsfile/2013/03/29/0640e5a7e0c8f86ff4a380150357bbef.pdf. Accessed on 24 September 2014.

[20] The European Chamber of Commerce in China (2015). ‘Internet Restrictions Increasingly Harmful to Business, say European Companies in China’, http://www.europeanchamber.com.cn/en/press-releases/2235/internet_restrctions_increasingly_harmful_to_business_says_european_companies_in_china. Accessed on 17 February 2015.

[21] Bradsher, Keith (2014). ‘Looking Beyond China, Some Companies Shift Personnel’, http://www.nytimes.com/2014/09/10/business/international/looking-beyond-china-some-companies-shift-personnel.html?_r=0. Accessed on 30 November 2014.

[22] Ricker, Thomas (2010). ‘Chinese iPhone approved with WAPI WiFi’, http://www.engadget.com/2010/05/04/chinese-iphone-approved-with-wapi-wifi/. Accessed on 30 November 2014.

[23] Shouji zhongguo wang 手机中国网 (2015). ‘苹果成全球首个接受中方网络安全审查的公司’ (Apple will be the world’s first company to have network security tested by the Chinese), http://t.m.china.com.cn/convert/c_uPId9W.html. Accessed on 22 January 2015.

[24] Mozur, Paul (2015). ‘New Rules in China Upset Western Tech Companies’, http://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html?ref=business&_r=0. Accessed on 2 February 2015.

[25] Brodkin, Jon (2011). ‘Ballmer to Hu: 90% of Microsoft customers in China using pirated software’, http://www.networkworld.com/article/2199038/software/ballmer-to-hu--90--of-microsoft-customers-in-china-using-pirated-software.html. Accessed on 30 November 2014.

[26] Gantz, John F. et al. (2013). ‘The Dangerous World of Counterfeit and Pirated Software’, white paper no. 239751.

http://news.microsoft.com/download/presskits/antipiracy/docs/IDC030513.pdf. Accessed on 22 October 2014.

[27] The Onion Routing (Tor). One way to circumvent Internet censorship.

[28] Heilmann, Sebastian (2014). 'Lob der Nischenpolitik – Deutschland spielt in Europas China-Politik heute die Rolle des Impulsgebers' (In praise of niche politics: Germany plays the part of the initiator in China's current policy'), *Internationale Politik*, September/October, 34–43.