CHINESE TELECOMMUNICATION COMPANIES:

Political and legal vulnerabilities and how Europe should deal with them

Frank N. Pieke, Katja Drinhausen, Mareike Ohlberg

KEY FINDINGS AND RECOMMENDATIONS

- Faced with technological unknowns, the selection of equipment and service providers for 5G infrastructure is a matter of political trust; Europe needs to decide whether to extend that trust to the Chinese party-state.
- Chinese national security legislation combined with actual political-legal practice mean that Chinese companies and individuals can be pressured by the party-state to grant access to critical infrastructure and information where it is technically possible.
- Huawei has been adamant in stating its independence and legal compliance, but Huawei's expert analysis leaves out the State Security Law, the key component of the national security framework.
- China itself regards national security as paramount and has extensive legislation in place to restrict access of foreign telecommunication technology providers.
- European governments should not extend political trust to China *prima facie* but conduct a qualified risk assessment that also takes the political environment and legal practice into consideration.

March 2019

merics
Mercator Institute
for China Studies

1. THE SELECTION OF EQUIPMENT AND SERVICE PROVIDERS IS A MATTER OF POLITICAL TRUST

When choosing equipment and service providers for critical information and network infrastructure such as 5G, European governments have to balance the protection of open markets and the benefits of competition against long-term risks where unwanted access by third parties cannot be effectively prevented. Regarding Chinese telecommunication companies such as Huawei and ZTE, the unease of security agencies does not seem to come from hard evidence of proven security breaches, but primarily from technological "known unknowns" and the difficulty in detecting illegitimate data flows in a timely manner and/or ruling them out reliably.

European member states need to decide if they are willing to trust the Chinese party-state not to abuse its power over companies and individuals to gain access to critical infrastructure and information

As discussed in a recent paper by the German Institute for International and Security Affairs (Stiftung Wissenschaft und Politik, SWP) the main issue is not whether providers of technological equipment are building in "backdoor" access to the network now, but rather that providers will have future access for network operation and maintenance purposes due to the fact that hard- and software cannot be clearly separated in 5G technology. This remote access could then be used to change the code in order to access infrastructure and information beyond the intended scope.

The main question is whether potential equipment and service providers of critical information and network infrastructure can be pressured by the government of their country of origin to abuse such access for the purpose of espionage or more direct interference in the future – in other words, a question about long-term political trust. While the US has been actively lobbying for an exclusion of Chinese telecommunication companies from 5G network construction and drawn China's criticism that this is mainly to contain the PRC politically and economically, the key concerns in Europe are – and should be – independent of such a geopolitical US push. European member states need to decide for themselves if they, in light of the overall political and legal environment in China, are willing to trust the Chinese party-state not to abuse their power over Chinese companies and individuals to gain access to critical infrastructure and information.

2. CHINESE LAW MAKES EVERYONE RESPONSIBLE FOR PROTECTING NATIONAL SECURITY

The vulnerabilities of Chinese telecommunication companies are rooted, in part, in national security legislation, most importantly the 2015 State Security Law. In 2014, the old State Security Law from 1993 was abolished and its main content transferred – in updated form – to the new Counterespionage Law. In 2015 a new State Security Law was adopted which, despite sharing the same name as the predecessor of the Counterespionage Law, is in fact much more wide-ranging. The new State Security Law establishes:

a) a broad concept of state security that also includes "sustainable economic and social development, and other major national interests" (art. 3),
b) CCP leadership over all national security work (art. 4) and
c) the obligation of all citizens, enterprises and other entities to cooperate with state organs to safeguard state security (arts. 11, 77).

Box 1

Relevant articles from the PRC State Security Law (2015)

[...]
Article 2 National security refers to the relative absence of international or domestic threats to the state's power to govern, sovereignty, unity and territorial integrity, the welfare of the people, sustainable economic and social development, and other major national interests, and the ability to ensure a continued state of security.
Article 3 National security efforts shall adhere to a comprehensive understanding of national security, make the security of the People their goal, political security their basis and economic security their foundation; make military, cultural and social security their safeguard and advance international security to protect national security in all areas, build a national security system and follow a path of national security with Chinese characteristics.
Article 4 All national security work shall adhere to the leadership of the Chinese Communist Party, and a centralized, unified, efficient, and authoritative national security leadership system shall be established.
Article 11 Citizens of the People's Republic of China, all state organs and armed forces, all political parties and mass organizations, enterprises, public institutions and other social organizations, each have the responsibility and obligation to preserve national security. [...]

Chapter VI: Duties and Rights of Citizens and Organizations
Article 77 Citizens and organizations shall fulfil the following obligations to preserve national security:
(1) obey the relevant provisions of the Constitution, laws, and regulations regarding national security;
(2) promptly report leads on activities endangering national security;
(3) truthfully provide evidence they become aware of related to activities endangering national security;
(4) provide conditions to facilitate national security efforts and other assistance;
(5) provide public security organs, state security organs or relevant military organs with necessary support and assistance;
(6) keep state secrets they learn of confidential;
(7) other duties provided by law or administrative regulations.

Individuals and organizations must not act to endanger national security and must not provide any kind of support or assistance to individuals or organizations endangering national security. [...]

The definition of national security in the law is closely related to Xi's concept of a "comprehensive national security outlook" which encompasses the fields of politics, territory, military, economy, culture, society, science and technology, information, ecology, nuclear and natural resources as key areas and has been criticized by foreign observers as so expansive that almost everything can be regarded as a matter of national security.

China's definition of national security has been criticized by foreign observers as so expansive that almost everything can be included

The State Security Law serves as the "umbrella" law for the Counterespionage Law, National Intelligence Law and Cybersecurity Law. What all these laws have in common is the premise that everyone is responsible for state security. According to the Canadian Security Intelligence Service (CSIS), social mobilization for counter-espionage, the global reach of Chinese companies and the explicit intelligence role in supporting economic growth are the hallmarks of China's new intelligence strategy.

As is often the case in China, the wording in the laws mentioned above is intentionally ambiguous in some areas to allow for flexible application. Even if the requirement for individuals and enterprises to cooperate with security forces is not explicitly stipulated in the laws and regulations, the broad requirements and ambiguity of terms can well be used to require and pressure enterprises to comply with requests to grant access where it is technically possible, even if it might conflict with other domestic or international norms and obligations.

Box 2

Relevant national security legislation

- *old* State Security Law of the PRC (February 2, 1993) [*replaced by the new Counterespionage Law in 2014*]
- Counterespionage Law of the PRC (November 1, 2014)
- State Security Law of the PRC (July 1, 2015) [*also translated as National Security Law*]
- Cybersecurity Law of the PRC (November 16, 2016)
- Detailed Rules for the Implementation of the Counterespionage Law (November 22, 2017)
- National Intelligence Law of the PRC (June 27, 2017)

3. THE CHINESE PARTY-STATE HAS INSTITUTIONALIZED CHANNELS FOR POLITICAL INFLUENCE

Additional risks of state inference lie in the institutionalized channels for political influence on businesses and the justice system in China. While private Chinese enterprises are not merely agents of the CCP and generally function largely independently both within China and in international markets, the Chinese party-state has implemented and recently expanded mechanisms (party committees, party cells and secretaries) to exert influence where it deems necessary. New party regulations clearly state the aim of expanding party committees (branches) and their role in the private sector. There have been numerous complaints from Western private enterprises to their governments about being “guided” by party committees. Therefore, it is reasonable for Western governments to assume that the CCP has the intention to influence and to use party committees or cells in at least some instances.

Within the judicial and law enforcement systems, the political-legal committees, party committees and secretaries fulfill a similar steering function that allows targeted political interference. The CCP’s hold over state institutions is likely to increase under the ongoing initiative to strengthen party leadership over the legal system. Independent oversight bodies over state security organs that citizens and enterprises might turn to if they receive undue requests for cooperation are de facto non-existent. This has facilitated the Chinese state’s and the CCP’s selective violation of domestic and international law as well as the sovereignty of other states to safeguard and assert their interests (a well-documented pattern that ranges from hostage diplomacy to detentions of dissidents and ethnic minority members).

One case that has cast suspicion was the ICT infrastructure of the African Union provided by Huawei. Between January 2012 and January 2017, data packages were sent to a server in Shanghai every night between midnight and 2 a.m. Even if there were no state involvement in the hacking of the Chinese-supplied African Union headquarters' computer systems uncovered in 2018 or the recent espionage allegations in Poland, these cases illustrate the vulnerability of both technology and individuals as potential points of access.

4. HUAWEI'S EXPERT ANALYSIS MISSES OUT A KEY PIECE OF NATIONAL SECURITY LEGISLATION

Due to Huawei's participation in bidding processes around the globe, it is at the center of current debates and has already been restricted in some markets. Both Huawei representatives and Chinese government and party officials have brought forward legal arguments to convince potential customers around the globe that private Chinese enterprises are independent of the state and that they cannot be compelled to grant the state access to sensitive information and critical networks. But the actions of the Chinese government in the aftermath of the arrest of Meng Wanzhou, Huawei CFO and daughter of founder Ren Zhengfei on December 1, 2018, such as the ensuing arrests of Canadians Michael Spavor and Michael Kovrig and the surprising death penalty for Robert Lloyd Schellenberg, have made clear that the Chinese government considers Huawei a Chinese asset.

To support the claim that the Chinese party-state cannot require Chinese telecommunication companies to provide access or privileged information of foreign states based on Chinese law, Huawei provided a legal analysis by Chinese law firm Zhong Lun ("Declaration of Jihong Chen and Jianwei Fang"). The expert analysis is correct in stating that Chinese law does not explicitly require telecommunication equipment manufacturers such as Huawei to cooperate with any request by the Chinese government "to use their systems or access them for malicious purposes under the guise of state security", nor does it explicitly authorize the Chinese government "to order manufacturers to hack into products they make to spy on or disable communications."

Nonetheless, the legal analysis has significant shortcomings as a basis for risk assessment. The expert analysis only examines relevant paragraphs in the Counterespionage Law, National Intelligence Law and Cybersecurity Law, while the new, wide-reaching State Security Law from 2015 – a key component of the national security framework – is not even mentioned. By giving the impression that the State Security Law was abolished without further replacement other than the more specific Counterespionage Law the expertise fails to address a key point of international concern. Moreover, the analysis consists of a narrow interpretation of formal law and does not take into account legal and executive practice. Such legal assessments only have value if the Chinese state reliably acts within the confines of the law.

5. CHINA RESTRICTS ACCESS OF FOREIGN TELECOMMUNICATION TECHNOLOGY PROVIDERS

For China, safeguarding national security is the top priority when choosing components and services for its own key communication infrastructure

For China, too, safeguarding national security is the top priority when it comes to choosing components and services for key communication infrastructure in China, as evidenced in a number of official statements. Even if the Chinese market were opened up further under the new Foreign Investment Law (expected to be adopted by the NPC in March 2019) and the telecommunications sector is declared open for foreign enterprises, the Foreign Investment Law, the Procurement Law (2014) and the Tendering and Bidding Law (2017) contain an exemption from regular proceedings where national security is involved. Moreover, a security review is automatically required for components and services for "key information infrastructure" under the Cybersecurity Law and the Interim Measures on the Security Review of Network Products and Services (2017).

The recent decision (January 2019) of Chinese regulators to grant British Telecom (BT) a Domestic IP-VPN license and a nationwide Internet Service Provider (ISP) license – the first ever licenses given to foreign telecommunication companies – do not constitute actual access to key information infrastructure as BT will have to rely on existing Chinese networks and will have to comply with strict data localization requirements under the Cybersecurity Law as well as provide access to data communicated via its services, including VPN. Further reports that China's big mobile network operators (China Mobile, China Unicom and China Telecom) have signed deals with Nokia and Ericsson to provide parts for China's 5G networks are equally to be seen as a symbolic show of good will rather than political trust, as the technologies and services will actually be provided via the two companies' Chinese joint ventures, which essentially are Chinese companies in their obligations towards the Chinese state.

6. RECOMMENDATIONS: WHAT EUROPEAN GOVERNMENTS SHOULD DO

- European governments should remain committed to free market principles, restricting access only as an extraordinary measure where there are plausible risks that cannot by contained by technical means.
- European governments should exchange information among themselves but also with allies (e.g. within the G7), specifically relating to security assessment and their respective arguments for or against restricting access to Chinese telecommunication companies.
- European ministries and departments responsible for cybersecurity should conduct a comprehensive risk assessment of technological vulnerabilities of 5G network architecture that makes best use of information including that from key allies, especially of potential future risks in as far these can reliably be known or expected.
- European governments should make their decisions on the inclusion or exclusion of companies from non-allied countries in 5G networks with common European interests in mind, particularly with a view to avoiding a "bifurcated" 5G world in Europe. The decision should be made independently from the United States.

- European governments should keep in mind that no-spy agreements only provide an effective means of protection if China is to be reliably expected to be constrained by international law.
- In deciding whether to trust the Chinese state not to abuse its legal and political power over Chinese private companies, European governments should:
  – seek independent legal opinions by international experts on Chinese law;
  – consider the political environment and legal practice in China, especially institutionalized channels for political influence and lack of independent oversight;
  – consider China's track record in adherence to international law and obligations where these are in conflict with its domestic security priorities;
  – consider the risks of the future development of economic and diplomatic relations with China;
  – consider China's own banning of fully foreign-owned telecommunication companies in 5G network and other key information infrastructure construction.
- If choosing to exclude companies from non-allied countries in critical infrastructure, European governments should not target individual companies but ensure that measures are based on transparent and reliable standards and procedures that distinguish between sourcing from EU partners or other allies and countries outside this circle.
- If choosing to exclude specific companies, European governments should stress that restrictions are based on special concerns regarding national security and data security of its citizens and are not intended to restrict Chinese companies' access to European markets to which they continue to be welcome.

Faced with technological unknowns, the selection of equipment and service providers for 5G infrastructure is a matter of political trust

Box 3

Selected sources and recommended reading

- Canadian Security Intelligence Service (2018). "China's intelligence law and the country's future intelligence competitions." May 17. https://www.canada.ca/en/security-intelligence-service/corporate/publications/china-and-the-age-of-strategic-rivalry/chinas-intelligence-law-and-the-countrys-future-intelligence-competitions.html. Accessed: February 15, 2019.
- Hoffman, Samantha, Kania, Elsa (2018). "Huawei and the ambiguity of China's intelligence and counter-espionage laws." September 13. https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/. Accessed: February 15, 2019.
- Voelsen, Daniel (2019): "5G, Huawei und die Sicherheit unserer Kommunikationsnetze." February 5. https://www.swp-berlin.org/fileadmin/contents/products/aktuell/2019A05_job.pdf. Accessed: February 15, 2019.
- Cave, Danielle (2018). "The African Union headquarters hack and Australia's 5G network." July 13. https://www.aspistrategist.org.au/the-african-union-headquarters-hack-and-australias-5g-network/. Accessed: February 15, 2019.

Imprint
MERICS | Mercator Institute for China Studies
Klosterstraße 64, 10179 Berlin, Germany
Tel.: +49 30 3440 999 0
Mail: info@merics.de
www.merics.de