SINOPSIS
CHINA IN CONTEXT AND PERSPECTIVE

Date: December 11, 2023

Understanding the risk of Chinese ICT companies: the Czech Republic's Perspective

Author: Project Sinopsis, Prague, the Czech Republic

Executive Summary

- Chinese ICT companies maintain extensive and permanent connections with the Chinese government and the Chinese Communist Party (CCP), including its intelligence services, law enforcement agencies, and the military.
- The legal framework in the People's Republic of China (PRC) compels Chinese ICT companies to actively engage in intelligence activities. In return, the Chinese government pledges protection for individuals and entities involved in such activities. The political structure of the PRC does not permit Chinese ICT companies to reject cooperation with state authorities.
- The State Intelligence Law is the most important law from the collection of state security acts in terms of defining the obligations of individuals and organizations to participate in state intelligence activities.
- The CCP tightly controls private companies' operations through the legally mandated presence of CCP cells in companies' structures.

- The inclusion of products from Chinese ICT companies in crucial governmental and Critical Information Infrastructure (CII) systems poses an exceptionally high risk. Neglecting these risks could result in significant adverse impacts on the national security of a given country.
- A Chinese vendor acting on behalf of or enabling the activity of the Chinese state security apparatus may pose a threat to confidentiality, integrity and availability of 5G networks.
- Security measures such as testing and certifications do not provide adequate security guarantees in the absence of trust in the supplier.
- The Czech Republic's approach helped to establish non-technical aspects of cybersecurity as equally important, driving trust-based risk assessment as a central focus in securing 5G networks.

Chinese ICT companies and the Chinese Party-State

Over the past two decades, Chinese information and communication technology (ICT) companies have risen to prominence as key global players, particularly in the research and development of innovative technologies. Their success can be attributed to a vast talent pool and substantial investments in research and development. Another contributing factor is the significant support from the government, involving heavy subsidies, and instances of industrial espionage where the Chinese government assisted both state-owned and private companies.

The political and legal context within the PRC emerges as a prominent and critical issue when added to the organizational and personal connections of Chinese ICT companies to Chinese Communist Party's (CCP) interests. Laws such as the State Intelligence Law, Company Law, or the Cyber Security Law, in tandem with the political framework in China, essentially do not permit Chinese ICT companies to reject cooperation in the PRC's espionage and surveillance activities and at the same time strongly incentivize such cooperation.

While many Chinese ICT companies may be officially considered private entities, the political framework within which they operate necessitates their compliance. The takeovers of Anbang Insurance[1] and CEFC[2] underscore this reality. The Chinese government's purchase of controlling equity stakes in companies like Tencent or

[1] China seizes control of Anbang Insurance as chairman prosecuted, https://www.reuters.com/article/us-china-anbang-regulation-idUSKCN1G7076/

[2] State-owned Citic takes over troubled tycoon Ye Jianming's investments in Czech Republic, https://www.scmp.com/business/companies/article/2142579/state-owned-citic-takes-over-troubled-tycoon-ye-jianmings

Alibaba[3] show that the Chinese state is willing to assume control of private companies that fall out of favor with the Communist Party's leadership. The hypothetical scenario of Huawei or ZTE refusing the Chinese government's request to engage in intelligence activities would likely result in a direct takeover of the company by the state, accompanied by severe penalties for its leadership.

The dynamic relations among the Chinese Communist Party (CCP), the state, and both state-owned and private companies extend beyond mere intimidation. Chinese ICT companies have been actively involved in the research and development of technology with military or internal security applications since their inception. These companies also recognize that they stand to benefit from government support, regardless of potential repercussions such as damage to their reputation abroad due to perceived or actual failures in safeguarding client information. Moreover, they can generally count on the principle of plausible deniability, making it challenging to conclusively prove any nefarious intent on the part of Chinese ICT companies. **Forming direct or indirect affiliations between ICT companies and the intelligence services, law enforcement agencies, and the military of the People's Republic of China (PRC) is further encouraged through military-oriented research and development under the umbrella of Military-Civil Fusion (MCF).[4]** A report dating back to 2012, commissioned for the US-China Economic and Security Review Commission (USCC), provides a comprehensive overview of People's Liberation Army (PLA) projects

[3] China to take 'golden shares' in tech firms Alibaba and Tencent, https://www.theguardian.com/world/2023/jan/13/china-to-take-golden-shares-in-tech-firms-alibaba-and-tencent

[4] The foundation of innovation under military-civil fusion: The role of universities, https://sinopsis.cz/en/mcf/

involving Huawei and ZTE at that time.[5] Given the ongoing trend of integrating civil and military sectors, it is likely that the involvement of ICT companies in military research has further expanded since the publication of the report a decade ago.

Obligation to Cooperate

Chinese authorities embrace a comprehensive definition of state security, departing from the conventional understanding of national security prevalent in the Euro-Atlantic region.

A distinctive feature of the Chinese approach to state security is the expectation that every citizen and organization actively contributes to the state security, as mandated by the laws of the People's Republic of China. The primary objective of legally obligating individuals to ensure state security is to uphold the continuity of the rule of the Chinese Communist Party (CCP).

The interconnection between the state and the Communist Party of China is absolute and, to a significant extent, tighter than observed in the communist regimes of the Eastern Bloc. The influence of the CCP over the PRC's state institutions has always been conspicuous. However, under the current leadership of Communist Party Chairman Xi Jinping, the control exerted by party bodies has further strengthened. Numerous state institutions previously under the jurisdiction of the PRC State Council (PRC Government) are now directly under the control of the Central Committee of the Communist Party. For example, the Cyberspace Administration of China was transferred from the State Council to party organs in 2014, and in 2018 the

[5] Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage, https://www.uscc.gov/Research/occupying-information-high-ground-chinese-capabilities-computer-network-operations-and. USCC is a commission created and funded by the US Congress to research and monitor US-China security and economic issues.

Central Cyber Space Committee of the Central Council of the Communist Party assumed superior authority over China's cybersecurity agency. [6]

A contributing factor to the risk profile of Chinese companies is the lack of genuine independence in the judiciary of the People's Republic of China (PRC), leaving little recourse for Chinese companies seeking legal protection against the demands of state authorities. PRC courts are obligated to consider the directives of the Communist Party of China and, simultaneously, are subject to oversight from the prosecutor's office and the people's assemblies (with the National People's Congress representing the highest level of people's assemblies). A significant factor is the considerable personal risk that Chinese business leaders would assume if they were to challenge state authorities (and consequently, the leadership of the CCP) in court. Nevertheless, such a scenario remains largely theoretical, as it is highly unlikely that any organization or individual would consider resorting to the judiciary to contest the government on matters related to state security.

The 2018 Warning and Huawei in the Czech Republic

On December 17, 2018, the National Cyber and Information Security Agency (NUKIB) of the **Czech Republic issued Europe's first-of-a-kind regulatory warning[7] against the use of technology from Chinese companies Huawei and ZTE.** In the fourth point of the rationale behind the warning, NUKIB highlighted the legal and political landscape of the People's Republic of China (PRC), emphasizing that Chinese companies are compelled to cooperate in advancing the interests of the PRC:

[6] Behind the Facade of China's Cyber Super-Regulator, https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/

[7] SOFTWARE AND HARDWARE OF HUAWEI AND ZTE IS A SECURITY THREAT, https://www.govcert.cz/en/info/events/2682-software-and-hardware-of-huawei-and-zte-is-a-security-threat/

The legal and political environment of the People's Republic of China ("PRC") in which the companies primarily operate and whose laws are required to comply with, requires private companies to cooperate in meeting the interests of the PRC, including participation in intelligence activities etc. At the same time, these companies usually do not refrain from such cooperation with the state; in this environment, efforts to protect customers' interests at the expense of the interests of the PRC are significantly reduced. According to available information, there is an organizational and personal link between these companies and the state. Therefore, this raise concerns that the interests of the PRC may be prioritized over the interests of the users of these companies' technologies.

NUKIB's concern was not only addressing confidentiality of data, but also its integrity and, more importantly in the case of telecommunications networks, the availability of future 5G networks. NUKIB remains concerned that Huawei or ZTE could, under the influence of Chinese state security institutions, disable key elements of Czech critical information infrastructure.

At the time of NUKIB's warning, Huawei had established a significant presence in the Czech Republic, particularly through its involvement in the infrastructure of the country's three major mobile operators: O2, Vodafone, and T-Mobile. A key factor prompting closer examination by the Czech security community into Huawei's activities was a public bid for constructing a data center for the state-owned energy company CEZ. Like mobile operators, CEZ is recognized as a critical information infrastructure entity and falls under the regulatory jurisdiction of NUKIB. In the case of the data center bid, all three of the lowest bids came from companies that were local partners of Huawei.[8] Critics of the tender argued at the time that the sole criterion considered was the bid price, pointing out that the bids from Huawei's partners were exceptionally low, raising concerns about their viability without potential subsidies from the Chinese company. This has led to speculation that Huawei's motives may not have been solely

[8] China's Huawei wants to get into ČEZ, it offered the best price of data centre equipment, https://www.lupa.cz/clanky/cinsky-huawei-se-chce-dostat-do-cezu-nabidl-nejnizsi-ceny-na-vybaveni-datacentra/

commercial in nature. As in many countries, public bidding law in the Czech Republic encourages the selection of bids with the lowest offer to incentivize saving taxpayers' money. The law includes national security provisions, but these are rarely invoked to avoid additional screening from the fair-competition watchdog. This is of course problematic behaviour in the case of a bidding agency or organization where national security considerations are proper and reasonable and the bid's financial value should not be the only determinative factor. The Czech Republic's intelligence community raised the issue in 2017, namely the country's **counterintelligence agency BIS noted in its annual report that Chinese companies have no difficulty in meeting the formal security requirements for participation in tender, even though they are associated with security risks arising […] from the strong links between these companies and the Chinese state and its foreign policy interests.**[9]

NUKIB's warning did not ban Huawei and ZTE technology. However, it elevated the threat level value to maximum for mandatory risk assessment for entities under the Czech Cyber Security Act (CSA). That act required organizations wishing to acquire new ICT equipment to implement costly protective measures should they choose Huawei or ZTE or opt for a different supplier. The warning incentivized national security considerations by making the often-cheapest Huawei offer potentially more expensive than that of its competitors because of the need to buy additional technological solutions whose only purpose was to watch how the Huawei kit functioned.

Nevertheless, while the warning served its purpose, a more permanent solution is needed. Currently, after a period of soliciting public comments and a mandatory review

[9] Security Information Service Annual Report 2016, https://www.bis.cz/vyrocni-zprava16e1.html?ArticleID=1136

by other government agencies, an amendment to the CSA seeks to establish a mechanism that would enable a ban on untrustworthy, high-risk suppliers**. In 2022, NUKIB, in cooperation with intelligence services and relevant government agencies, issued "The Recommendation for assessing the trustworthiness of technology suppliers of 5G networks in the Czech Republic"[10] that outlined key priorities of the Czech Republic's national security community[11] in selecting suppliers for critical information infrastructure such as 5G networks, namely that the supplier should come from a country with a democratically elected government, an independent judiciary, and one that is not engaged in activities counter to the Czech Republic's or its allies' interests.**

Chinese laws relevant for NUKIB's 2018 Warning against Huawei and ZTE

State Security Law (2015)

The People's Republic of China (PRC) revised its state security legislation between 2014 and 2017, introducing the State Security Law (国家安全法) in July 2015. Articles 4 and 15 explicitly acknowledge the leadership role of the Communist Party of China in matters of state security. Article 77 delineates the responsibilities of citizens and organizations concerning state security:

> 1) Complying with the relevant provisions of the Constitution, laws, and regulations pertaining to national security.

[10] The Recommendation for assessing the trustworthiness of technology suppliers of 5G networks in the Czech Republic, https://www.nukib.cz/en/infoservis-en/news/1805-the-recommendation-for-assessing-the-trustworthiness-of-technology-suppliers-of-5g-networks-in-the-czech-republic/

[11] Loosely defined as organizations tasked with protection of national security like intelligence agencies, national policy, NUKIB, and ministries of interior, defence, and foreign affairs.

2) Promptly reporting information on activities that pose a threat to national security.

3) Truthfully providing evidence related to activities endangering national security.

4) Offering conditions to facilitate national security efforts and providing other forms of assistance.

5) Supplying necessary support and assistance to public security organs, state security organs, or relevant military organs.

6) Safeguarding the confidentiality of state secrets they become aware of.

7) Fulfilling other duties as stipulated by law or administrative regulations.

The State Security Law establishes a general obligation for citizens and organizations to assist state authorities in matters of state security. Subsequent laws build upon this broadly defined obligation, tailoring it to the specific activities outlined in each respective law.

State Intelligence Law (2017)

The State Intelligence Law is the most important law from the collection of state security acts in terms of defining the obligations of individuals and organizations to participate in state intelligence activities. **Article 7** defines the obligation of entities and their protection by the state:

All organizations and citizens are required by law to support national intelligence work, to cooperate, and to keep secrecy about the secrets they learn in connection with national intelligence work.

The state protects individuals and organizations contributing to the support and cooperation in the context of national intelligence work.

Article 14 of the law emphasizes that the relevant state institutions are entitled to require cooperation from individuals and organizations:

National intelligence services may, in accordance with related state regulations, request the competent authorities, organizations and citizens to provide the necessary support and cooperation.

For obvious reasons, the law does not mention foreign intelligence, but cases of participation by private companies in intelligence activities are known.[12]

Companies Law (2013)

In contrast to the previously mentioned laws, this regulation does not directly pertain to state security. However, Article 19 introduces a mechanism for the influence of the Communist Party on companies:

A Chinese Communist Party organization will be established within the company to conduct Party activities in accordance with the Constitution of the Chinese Communist Party. The company is required to facilitate the necessary conditions for the functioning of the party organization.

The obligation to establish a party cell is not a recent development. Following Xi Jinping's assumption of leadership in both the Party and the state, this rule has been more rigorously enforced, with the Communist Party of China (CPC) frequently holding positions in the top echelons of ostensibly private companies. Regarding the obligation

[12] For example: U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage, https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations

of citizens and organizations in the People's Republic of China (PRC) to participate in intelligence activities, stemming from the broad interpretation of the obligation to ensure state security, it is crucial to examine the mechanisms through which the Communist Party of China influences nominally private companies, such as Huawei or ZTE.

According to information from open sources, as early as 2007, when the presence of party cells was not strictly mandated in nominally private companies, Huawei already had 56 major party cells and 300 lower-level cells involving 12,000 employees. The current leader of the party organization at Huawei, Zhou Daiqi (周代琪), also holds the position of Senior Vice President of Huawei, representing the company at the highest level.

Australian inspiration

While the Czech Republic's warning was the first time an EU member state took regulatory measures against Chinese ICT companies, the approach that Czech authorities took can be tracked to the Australian decision to ban Huawei and ZTE from 5G networks just three months earlier. In late August 2018, the Australian government made the decision to exclude Huawei and ZTE from future development projects of 5G networks. Although the government's decision does not specifically name Huawei or ZTE, it states in the key part:[13]

> *The Government considers that the involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with*

[13] Government Provides 5G Security Guidance To Australian Carriers, https://www.minister.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers

> *Australian law, may risk failure by the carrier to adequately protect a 5G network from unauthorised access or interference.*

This constitutes a clear reference to the provisions outlined in Articles 7 and 14 of the Chinese State Intelligence Law. While Canberra did not explicitly specify Chinese ICT companies in its decision, it is evident that Huawei and ZTE meet the criteria. The Australian government can invoke the Telecommunications Sector Security Reforms (TSSR) as the legal basis for its determination.

Another argument put forth by the Australian authorities asserts that, unlike previous network generations, 5G networks lack a distinct division between core and peripheral components. [14] Essentially, the Australian government contended that in 5G networks, it is impractical to mitigate risks by restricting problematic companies from the core systems. They posit that unlike the existing 4G/LTE (and older) networks, the 5G network cannot be segmented into a core where problematic vendors are prohibited and an access network where they can operate.

Inadequacy of Technical Safeguards: from warning to strategic measures

One of the most significant contributions of NUKIB's warning is that it elevated trust, or lack thereof, in the supplier on the level that was previously dominated by technical measures for securing a telecommunications network.

In May 2019, NUKIB convened the first Prague 5G Security conference that resulted in a series of recommendations known as Prague Proposals (PP). On the role of non-technical measures, PP stated:

[14] Ditto

Cyber security cannot be regarded as a purely technical issue. A safe, secure and resilient infrastructure requires adequate national strategies, sound policies, comprehensive legal framework and dedicated personnel, who are trained and educated appropriately. Strong cyber security supports the protection of civil liberties and privacy.

When dealing with cyber security threats, not only their technical nature, but also specific political, economic or other behaviour of malicious actors which seek to exploit our dependency on communication technologies should be taken into account.

Emphasis on non-technical aspects of cybersecurity stemmed also from a lack of trust in the adequacy of known technical solutions. Testing equipment for vulnerabilities in specialised centers for network devices, followed by certification, has been proposed as a strategy to alleviate security risks during their operation. Huawei offered its facilities for testing and in 2019 opened a "Huawei Cyber Security Transparency Centre" in Brussels.[15] Typically, network components undergo testing prior to deployment. However, these devices are not impervious to change, and each undergoes continuous updates for various reasons after the initial testing phase. A firmware update might rectify a vulnerability or potentially introduce a new one. This principle generally holds true for equipment from any manufacturer. The complexity escalates for ICT companies with legal obligations to act in the interest of their home country's government, significantly amplifying the potential for the misuse of their technologies beyond the standard risks associated with ICT. These constraints seriously undermine the effectiveness of test centers. The most critical shortcomings are:

- Testing centers provide a highly restricted capacity to monitor and alleviate the risks associated with the deployment of information and communication technologies (ICT). The primary challenge lies in the practical impossibility of

[15] Huawei Cyber Security Transparency Centre Opens in Brussels, https://www.huawei.com/en/news/2019/3/huawei-cyber-security-transparency-centre-brussels

guaranteeing that the equipment subjected to testing remains non-harmful following software and hardware updates.

- When testing centers are established by suppliers (e.g. Huawei) without independent oversight, the level of transparency relies entirely on the willingness of these companies.
- Product testing is exceptionally time-consuming. The source codes of devices can be exceedingly extensive, and the devices themselves comprise numerous components and electronic circuits with diverse functions. It is enough for one component of a particular device to engage in harmful activity under specific circumstances.
- Lack of credible guarantees that the products undergoing testing are identical to the components deployed in full operation. Simultaneously, these components may differ from those delivered to all customers, particularly operators of critical information infrastructure (CII).

The essence of NUKIB's warning and the core messaging of Prague Proposals eventually found its way into the European Union's 5G Security Toolbox released in January 2020. In addition to technical measures (TM), the Toolbox also included a set of strategic measures (SM) and supporting actions (SA).[16] Strategic Measure 3 (SM03) formulates the Czech Republic's contribution to 5G security: "Assessing the risk profile of suppliers and applying restrictions on suppliers considered to be high risk - including necessary exclusions to effectively mitigate risks - for key assets."

[16] Cybersecurity of 5G networks EU Toolbox of risk mitigating measures, https://ccdcoe.org/uploads/2020/01/EU-200129-Cybersecurity-of-5G-networks-EU-Toolbox-of-risk-mitigating-measures.pdf

Conclusions

The decision regarding technology suppliers for 5G telecommunication networks is one that will have a fundamental impact for years to come, especially as 5G reaches its full potential by the end of decade. As a technology, it will power some of the most critical functions in every country, including autonomous public transportation or the next generation of industrial processes. Choosing a trusted supplier is of paramount importance. Chinese companies offer technologically advanced and competitive solutions, but the political and legal environment in which they are both forced and content to operate means that they cannot be trusted with our future. Disregarding even the most basic risks stemming from Huawei's relations with the Chinese party-state could have severe consequences for national security and sovereignty.

Sinopsis is a Czech Republic based project implemented by the non-profit association AcaMedia z.ú., in scholarly collaboration with the Department of Sinology at Charles University in Prague. It aims to present a regular overview of developments in China and its impacts on the outside world from the perspectives of Czech, Chinese, and international observers.