

Huawei in Central and Eastern Europe: From Strategic Partner to Potential Threat

Written by Filip Jirouš and Jichang Lulu

This PDF is auto-generated for reference only. As such, it may contain some conversion errors and/or missing information. For all formal use please refer to the official version on the website, as linked below.

Huawei in Central and Eastern Europe: From Strategic Partner to Potential Threat

<https://www.e-ir.info/2019/05/19/huawei-in-central-europe-from-strategic-partner-to-potential-threat/>

FILIP JIROUŠ AND JICHANG LULU, MAY 19 2019

Central and Eastern Europe (CEE) came back to the center of the global debate on Huawei with the recent Prague 5G Security Conference's emphasis on "transparent ownership, partnerships, and corporate governance structures" and its recommendation to take into account the "model of governance" of third countries when assessing their "risk of influence" on information and communications technology (ICT) suppliers. The tech giant has been a hot topic in the region since a warning against its equipment was issued by the Czech National Cyber and Information Security Agency (NÚKIB) last December, which added heat to the ongoing discussion on PRC activities. The debate on the company's involvement in cyber and industrial espionage, and its connections to the Chinese state (including the Xinjiang surveillance state) escalated after the Canadian authorities arrested Meng Wanzhou, the company's Chief Financial Officer and the daughter of its founder, last December. This renewed focus created a window of opportunity for security circles to push against a company they had been warning against for years.

While the link between Huawei and the Chinese Party-state has received attention elsewhere, it remains little reported in CEE. Yet the region is a rather important part of the story and might prove to be a crucial battlefield for NATO and the EU's relationship with China. The deployment of "lawfare" and United Front tactics shows the importance the Chinese Communist Party (CCP) attaches to the struggle to keep its "national treasure" well-entrenched in the post-communist European states. Both lawfare (the use of local legal systems to advance PRC policy goals) and United Front work (the cultivation of local entities to co-opt them as allies) are classic tools the CCP employs in its activities abroad. Although it is hard to generalize in such a diverse grouping of countries, the CCP and Huawei's "elite capture" methods have yielded some successes, most recently illustrated by Czech President Zeman's willingness to lobby on behalf of Huawei ahead of the Prague 5G Conference.

The effectiveness of these influence activities often depends on the resilience of local institutions and civil society and the freedom of the media. In some countries, these activities have encountered little debate, eclipsed by local issues or other external security threats such as Russia. The Chinese Party-state's mobilization of all its available assets to defend Huawei's interests against local concerns shows, however, that China attaches great priority to these developments. An assessment of the PRC's relationships with CEE countries should, therefore, treat Huawei's ongoing battle as seriously as the CCP does, recognizing its interrelatedness with the Party-state's larger political influence goals. This article, based on our previous work on Huawei featured in Sinopsis' ongoing coverage, interviews with officials and new sources in Chinese and local languages, seeks to contribute to an evidence-based discussion of the security implications of the involvement of PRC suppliers in ICT infrastructure. It summarizes recent developments in some CEE countries vis-à-vis Huawei and the PRC, including new evidence of Huawei's links to the CCP, as well as an overview of the Baltic countries' reactions to the Huawei controversy, so far underreported in English.

"Economic Diplomacy", Geopolitics and Lawfare: Huawei as the Party-state's Champion

Huawei's battle for CEE cannot be isolated from the Party-state's recent inroads into the region, notably characterized by political influence activities. Large enterprises are a component of China's Party-led system, which embeds capitalist forces into a Leninist governance model. The Party-state's leverage on state and privately-owned

Huawei in Central and Eastern Europe: From Strategic Partner to Potential Threat

Written by Filip Jirouš and Jichang Lulu

enterprises and the overlap between national and business interests give even privately-owned “national champions” a role as policy tools.

In Huawei’s case, the links to the Party-state are particularly clear. In addition to chairman Ren Zhengfei’s PLA past, one must add the intelligence background of Sun Yafang, Ren’s former deputy. Huawei cooperates with the PRC’s law enforcement, notably in Xinjiang, the CCP’s “digital Leninism lab”. In contrast to the attempts to downplay the significance of Ren’s CCP membership to foreign audiences, the importance of Party work within the company has been repeatedly made clear. As Chairman Ren once put it: “We are a Chinese company, we support the Chinese Communist Party.” A 2017 article on private enterprise Party work (funded under a Shenzhen CCP Organization Department project) noted that the “core members” of Huawei’s teams abroad, including “the complex and difficult European market”, mostly consisted of Party members. Although Party work in private companies has been increasingly stressed under Xi Jinping’s tenure, Huawei already had 38 Party branches in 2000, which had grown to 300 by 2007, long before Xi’s rise to power. In 2012, Huawei’s system of Party committees was transformed into “offices of ethics and compliance” (OEC) under a “committee of ethics and compliance (CEC), whose roles, as Alex Joske, a researcher at the Australian Strategic Policy Institute, has noted, continue to include Party work. While membership is open up to non-Party members and even foreigners, chairman Ren has said that Party-members should reflect about their leading role if they got voted out of OECs. Huawei’s Party secretary is described as its top “ethics and compliance” officer on Huawei’s website, but multiple Chinese-language sources refer to his CCP role. Dual Party branch-OEC appointments can also be observed at lower levels in the company, and logos and internal materials of some Huawei OECs feature a hammer and sickle. PRC companies and other organizations often set up Party branches abroad; examples in CEE include Rongsheng in the Czech Republic and Liugong [?] in Poland. The 2017 Shenzhen article states that Huawei has also set up overseas Party branches. Given the political content of some OEC meetings abroad, these might overlap with the company’s overseas OECs, such as the one in Prague, whose chairman indeed calls himself a CCP member. This new evidence thus helps establish Huawei’s organic links to the CCP, and its efforts to obscure them as signs of a systemic lack of transparency. Huawei’s status as a component of the CCP-led system means that its activities abroad cannot be effectively separated from the interests of the PRC Party-state.

The CEE is an important market for Huawei, which might help explain the swift reaction to the recent setbacks. The region is also of interest to the CCP’s geopolitical initiatives, notably the “16+1” platform, a Beijing-led grouping of 16 CEE countries (Kosovo excluded, since the PRC does not officially recognize the young republic). These countries have little more in common than their Communist past, and the recent addition of Greece, effectively creating a “17+1”, makes these differences even starker. The CCP seems to see this arbitrary grouping of states with disparate histories and international affiliations as an easier political target than the rest of Europe. Some countries in the group show a tendency for strongman politics, closed-door deals, shady business practices while civil society and democratic institutions are often weaker than in Western Europe. The CCP might be better prepared to work with states with shorter democratic experiences and at times oligarchic restructuring of the economy after privatization. Besides its economic significance as a potential new trade route, the region could be seen as opening political doors into Europe and NATO, of which many of the CEE countries are current or prospective members. Indeed, while a narrative of “economic diplomacy” has been invoked in messaging promoting regional engagement with the CCP’s initiatives, CEE countries have seen little benefit in terms of trade and investment. The CCP has, however, been able to claim some successes in terms of propaganda and political influence.

The deployment of organs of the PRC Party-state and some of its local allies in defense of Huawei after the recent security warnings, using such time-honored CCP practices as propaganda and “lawfare”, illustrates the overlap between the interests of the Party and one of its tech champions.

The Czech Warning

Although Czech intelligence had expressed concerns about Huawei as early as 2014 and continued to do so for years, it was the warning last December by the cyber-security bureau NÚKIB (Národní ústav pro kybernetickou a informační bezpečnost) that triggered Czech action and a PRC response. The Czech state’s reaction to the NÚKIB’s warning saw the government instruct institutions and SOEs to finish conducting security checks by late May.

Huawei in Central and Eastern Europe: From Strategic Partner to Potential Threat

Written by Filip Jirouš and Jichang Lulu

Financial regulators excluded Huawei from procurement in a new tax system, and the Ministry of Defense directed its employees to get rid of a security app if they owned Huawei phones. The Prague mayor, from the opposition Pirate Party, soon announced he was also keen to investigate the risks posed by Huawei to city institutions.

The Czech debate on Huawei and, more generally, the PRC's influence, has been more heated than in the rest of the region. Anti-Communist sentiment among many in politics and civil society may be seen as one of the factors affecting China's image in the country. The relatively high level of support for Tibet, demonstrated once again during the leader of the government-in-exile's recent Prague visit, can serve as an illustration. Unfavorable public opinion, compounded by the risk of contagion of Huawei skepticism to the rest of the region, provide the background for the PRC's high-profile attempts to counter the Czech warning.

The Party-state apparatus was openly engaged in defense of Huawei. After an urgent pre-Christmas meeting with PM Andrej Babiš, the Chinese embassy summarized the conversation as the Czech Republic disowning the NÚKIB warning as a "mistake". Babiš dismissed the summary as lies. The PRC propaganda system was also mobilized against the Czech warning, with major state media outlets amplifying the official "mistake" story with a speed and interest seldom dispensed to a small European country. The Chinese Ministry of Foreign Affairs, state media, and Party organs would also be unusually quick to support the "friendly" Czech voices that soon rose to Huawei's defense.

Czech politics and business include several prominent actors long cultivated by the CCP-led global influence apparatus, in an "elite capture" process which has been investigated by Sinopsis for years. Under Xi Jinping, the CCP has turned United Front work, a set of co-optation tactics whose roots go back to Lenin, into a global political influence endeavor central to the world's politics, marshaling the CCP's dedicated institutions and a range of government, private and mixed entities. Notably, Czech president Miloš Zeman has become an advocate of pro-CCP policies, in particular openly attacking local security services for spreading "fake news" about Russian and Chinese espionage. Zeman owes some international notoriety to his association with the energy conglomerate CEFC, a company which, together with its non-profit arm, was involved in global influence operations until a bribery investigation led to its demise. Another favorite CCP interlocutor is the leader of the small but influential Czech Communist Party, which frequently interacts with the CCP's International Liaison Department.

During the Huawei saga, the CCP could count on the support of both these targets of "friendly contact" work. The Communist leader defended the company in January after a "private" fact-finding mission to China during which he was hosted by Huawei executives and Party officials. Also in January, President Zeman spent much of his weekly TV interview arguing the company's case against local scrutiny. Later that month, he met with local Huawei representatives. The message was again underlined during Zeman's April visit to the Belt and Road Summit in Beijing when he also met Huawei founder Ren Zhengfei and proclaimed that the Czech position in the Huawei case was "servile" toward a "campaign without evidence" against the company. Referring to what he saw as a contrast between the Czech and other European positions, he called his own country "a ferocious red speck on the map of the EU". The simile was inspired by a poorly drawn map, produced by Huawei itself, which shows a red Czech Republic standing out among its presumably pro-Huawei neighbors. The president attached the "red speck" map to an official letter in which he tried to lobby the Prime Minister to invite Huawei to the Prague 5G Security conference, where 32 countries were to agree on a rather Huawei-unfriendly set of recommendations. Huawei's leadership, Zeman wrote, had just "confirmed their interest in participating."

Besides the support of local co-opted elites, Huawei's response employed another tactic from the CCP's toolbox: lawfare. The company's PR operations in the Czech Republic and beyond have been touting a "legal opinion" by a British law firm as a proof that Huawei would not be obliged to cooperate with the PRC's security apparatus. The document, first discussed by Sinopsis, is in fact explicitly not to be taken as a "legal opinion". It is a review of an old piece of legal advice written by Chinese lawyers, one of them also an "outstanding lawyer Party member". The Chinese advice had already been unsuccessful in the US and Australia. When it was taken to the US again after the European deployment, it was met with a detailed rebuttal by an expert in Chinese law. These "lawfare" activities were accompanied with a vow to sue the Czech state over the NÚKIB warning. As Ondřej Klimeš, a Czech sinologist, has noted, these tactics resemble "public opinion warfare" and "legal warfare", two of the "three warfares" originating in

Huawei in Central and Eastern Europe: From Strategic Partner to Potential Threat

Written by Filip Jirouš and Jichang Lulu

PLA doctrine and generalized to civilian propaganda.

Spy Drama in Warsaw

In neighboring Poland, a Chinese Huawei executive and a Polish former intelligence agent were arrested in January under suspicion of cooperating with Chinese intelligence. On the same day the news became public, a Polish official announced the government was considering issuing a warning against Huawei, adding that “certain companies” could be “excluded from the Polish IT market”. As Łukasz Sarek, a Polish China researcher and market analyst, has noted, an analysis of the detained former Polish agent’s career shows he was in possession of valuable knowledge about Poland’s telecommunications infrastructure, in particular, an encrypted communications system for government officials. Compared to the Czech case, Huawei and the PRC’s reaction was relatively subdued in Poland: the company promptly fired the arrested executive and state media attacks were mostly confined to the predictably bellicose *Global Times*. The arrest of the two suspects was recently extended until July.

Even before the arrest of its executive, it was clear that Poland, the largest market in CEE, was a crucial battlefield for Huawei in the struggle to avoid getting locked out of Europe, perhaps one of the reasons behind the swiftness of the reaction to the Czech intelligence warning. Huawei has a strong presence in the Polish market, with multiple public institutions among its customers. Poland is key to Huawei’s 5G plans in Europe, with the company having conducted trials with both Orange and Deutsche Telekom. Despite the open skepticism aired in January, the Polish government has not excluded Huawei from 5G plans, with press reports quoting officials as suggesting that a “blanket ban” wouldn’t be economically feasible. After stalling on a decision for a month in what was already being labeled “the first exclusion of Huawei equipment in Poland”, a state research institute focused on Internet security chose Huawei last month for a network infrastructure project.

Huawei’s image tactics in Poland resemble those it has applied elsewhere. Like in the Czech Republic and Slovakia, the company has misrepresented the law firm declarations it commissioned as “independent legal opinions”. Huawei recently hired a former aide to premier Mateusz Morawiecki, a decision worth analyzing in the context of the company’s elite recruitment practices. Examples of such practices can be seen in its recruitment of former officials and political in the UK, its travel funding and other sponsoring of parliamentarians and media in Australia and New Zealand, its investment in Western think tanks, or the controversy over the presence of a Huawei employee at the European Network and Information Security Agency.

Strategic Partner or Potential Threat?

Even without the high-stakes drama playing out in Prague and Warsaw, concerns about Huawei’s security have been aired in other countries in the region. On the other hand, some governments do remain outright supportive towards the company.

In February, Lithuanian intelligence named the PRC in their annual threat assessment, with an official adding during a press conference that they were analyzing the security of the use of Huawei equipment but had no grounds to issue a warning against it. The PRC embassy protested the intelligence assessment in a strongly worded statement, and the ambassador would later raise the Huawei issue during a meeting with the Prime Minister in March. The defense ministry has said national defense systems will not use Huawei equipment. Latvian intelligence called in February for increased attention to possible Chinese espionage, without mentioning Huawei. While media coverage was avoided, a Latvian official told us in April that unspecified measures had been taken against potential risks posed by Chinese ICT technology. The latest Estonian Foreign Intelligence Service yearbook, issued in early March, says Huawei “has not convincingly proved” it’s not bound by law to collaborate with PRC intelligence work, and calls for risk analysis “in order to avoid dependency that could potentially be a security threat to both the public and private sector”. Despite these signs of caution, no general public warning comparable to the Czech one has been issued against Huawei in the Baltics. This might be due to the fact that the Czech warning has legal power because of the strong national cyber security law, which, according to a Czech official with knowledge of the matter, is comparatively stronger than in the rest of CEE. Both Lithuanian and Latvian telecom companies denied in February that cooperation with Huawei was endangered.

Huawei in Central and Eastern Europe: From Strategic Partner to Potential Threat

Written by Filip Jirouš and Jichang Lulu

Huawei's presence in Hungary includes its European production and logistics center. The company held its 2017 smart city summit in Budapest. Hungary is the largest recipient of Chinese investment in the region, with estimates ranging from 2.6bn to 3.3bn USD. Huawei's standing in the country seems unaffected by recent concerns, since Finance Minister Mihály Varga referred to Huawei as "a strategic partner of the government" in April.

The company's position also seems safe in Serbia, where agreements with Huawei have ranged from investment in telecom infrastructure to the smart and safe cities. Plans to install thousands of Huawei surveillance cameras have, however, raised some eyebrows.

Romania's main opposition party joined the ranks of critics of the Chinese company last March, calling for banning Huawei products from critical infrastructure and barring it from 5G development. While the government's first reactions were vague, the local Special Telecommunications Service (STS) has denied that Huawei equipment was present in critical infrastructure. The institution also noted it had not been consulted during the drafting of a 2013 memorandum of understanding between Huawei and the Romanian government, revealed by local media in 2014, that contemplated the company's involvement in the construction of ICT infrastructure.

Technological Expansion and Political Influence

CEE has become a key battlefield for global influence through technological expansion. China's Leninist system subsumes economic and technological development under the CCP's political goals. Huawei's status as a national champion and its links to the Party-state make it impossible to separate the company's forays from the PRC's national interest. The deployment of multiple strategies and actors is a clear sign of the importance the CCP attaches to the controversy. Huawei's opinion-management and "lawfare" tactics display the lack of transparency that characterizes the governance model of the system it belongs to. Its elite recruitment and lobbying practices resemble the CCP's United Front tactics, seeking to co-opt the elites of target nations. Huawei's interactions with CEE nations often mirror the Party-state's, with both similarly calibrated to local attitudes towards China's global influence. Both the company and the Party make use of co-opted members of the Czech elite, who can be relied upon to openly attack the country's own security services; lacking comparable leverage, both were cautious in their response to Poland's arrest of an executive. The company's position seems safer in Hungary and Serbia, whose governments are particularly friendly towards Xi Jinping's regional initiatives, than in Romania or the Baltics, where security concerns could play a larger role in public discourse.

Local attitudes thus range from views of Huawei as a "strategic partner" to concerns about its potential risks, correlating with trends in each country's debate on the relationship with the PRC as a whole. Discussing Huawei as part of a larger debate on the PRC is not, in fact, a mistake. As we have seen, the company's Party-state links effectively make any partnership with it a partnership with the CCP. The analysis of the implications of such a partnership should therefore consider the global interests of the CCP-led system, since they are inseparable from those of one of its components.

The recent 5G Security Conference's stress on both the "technical and non-technical nature of cyber threats", suggesting perhaps an emerging recognition of the linkage between the Party-state and its tech champions, put Prague once again at the center of Huawei and the CCP's global expansion. Their displeasure at not being among the thirty-two countries invited, conveyed through the crudely drawn map attached to Zeman's letter, is only the latest sign that the Party-state considers the matter "non-technical" as well.

Notes

Special thanks to Alex Joske, Ondřej Klimeš and Łukasz Sarek for insightful discussion and other help during the preparation of this article.

Huawei in Central and Eastern Europe: From Strategic Partner to Potential Threat

Written by Filip Jirouš and Jichang Lulu

About the author:

Filip Jirouš studies Sinology at Charles University, where he focuses on United Front work in the Czech Republic. In his collaboration with Sinopsis.cz, he has worked on Chinese technology, cybersecurity, Digital Leninism and Xinjiang.

Jichang Lulu is an independent researcher with an interest in China's activities abroad.