The Middle East Program

China's Foothold in Türkiye's Digital Ecosystem: Report Summary

Marianna Serveta

This study examines China's foothold in Türkiye's digital ecosystem. It also reflects on the risks associated with this foothold for Türkiye itself and for its Western allies.

In modern times, Sino–Turkish relations have been shaped by ideological rivalry. Despite multiple points of contention and periodic strains, the countries' economic and military bonds have never broken entirely. The last fifteen years have witnessed a deepening of that bond, marked by formalised cooperation under a strategic partnership, and an increasingly noticeable Chinese footprint across multiple sectors in Türkiye, including the digital sector. China's increased footprint has been facilitated by Türkiye's engagement with China's Digital Silk Road initiative and related actions on digital transformation. The digital sector's significance lies in its transnational character. Digital systems and technologies are not confined to the borders of the country that hosts them, but affect broader technological networks they are embedded in. So too does Chinese influence, which through digital networks could take on a transnational character. This signifies this topic's relevance for Swedish interests and security, both due to Sweden's NATO membership and the strengthened cooperation potential with Türkiye and Swedish business presence there.

Previous research that examines Chinese investments and business engagement has focused primarily on countries that view China as a geopolitical adversary. The case of Türkiye stands out: although the country is a NATO member, it has chosen to deepen its ties with China, and has welcomed Chinese engagement in sensitive sectors. Its progressively maturing cybersecurity environment suggests that Türkiye generally considers digital technologies pertinent to security and thus the digital domain potentially vulnerable. The fact that Ankara does not view Beijing's interest in and engagement with its digital ecosystem as inherently threatening, and rather encourages such engagement, resonates with Ankara's broader pursuit of strategic autonomy. In a Turkish context, this means the ability to independently assess its threat landscape and act according to its own interests, unhindered by ideological or institutional constraints.

This study's theoretical point of departure is that of weaponised interdependence. This implies that China, if it wishes, as a state with an advantage in power and resources, can exploit and weaponise its companies' position in Türkiye's digital ecosystem to coerce its adversaries. These could be Türkiye itself in times of worsened bilateral ties, or Turkish allies that China can reach through Türkiye's digital ecosystem.

The study identifies 151 Chinese companies as active within telecommunication infrastructure, economic platforms and financial technology, cloud computing and smart-city infrastructure, the units that form Türkiye's digital ecosystem. To analyse how Chinese companies engage with Türkiye's digital ecosystem and therefore assess their future activity ambitions as well as their influence potential, this study examines key investments and cooperation agreements as channels of engagement. Presenting a selection of those illustrates the varying extents of Chinese companies' entrenchment in Türkiye's digital ecosystem.

Türkiye's telecom sector exhibits clear signs of Chinese companies owning or exercising operational control over its infrastructure. Chinese firms and their technologies have become deeply integrated into Türkiye's telecom through infrastructure projects, investments, and partnerships with all major Turkish telecom operators. Chinese engagement spans developing AI-supported next-generation networks, technology and infrastructure deployment in Türkiye's hardware, and integrating telecom services, using Türkiye as a potential base for wider regional operations. A key factor behind this entrenchment is Chinese ownership in *Netaş*, Türkiye's leading Information and Communication Technology services provider, which has enabled Chinese technology to penetrate digital sectors and gain insight into critical infrastructure including airports, ports, and the banking sector. The extent of Chinese engagement exemplified in this study indicates a strong and growing Chinese foothold in Türkiye's telecom infrastructure, with

FOI Memo 9027
Project no: A12504
Approved by: Mike Winnerstig

December 2025

FOI

ongoing commitments that may lead to future lock-ins to Chinese technologies and standards.

Chinese engagement with Türkiye's digital sector is extensive and multifaceted, comparable to its deep engagement in infrastructure. In e-commerce, major investments have given Chinese firms comprehensive oversight of Türkiye's critical digital infrastructure. The example of Alibaba's activity is telling: the Chinese company has gained access to Turkish consumer and merchant data, logistics networks, and payment systems. These ventures not only expand China's economic footprint but also embed its technological standards into Türkiye's digital infrastructure. In fintech, Alibaba's partnerships with Turkish banks and fintech companies have enabled the integration of its payment system into Türkiye's financial network, linking it to China's global digital ecosystem. Particularly in e-commerce, Chinese engagement drives upscaling and expansion, reflecting a long-term commitment and the ability to shape the sector as a whole.

In cloud computing, Chinese companies are strengthening their foothold. Through long-term cooperation agreements and partnerships, Chinese companies have embedded their technology stacks into Turkish firms' core infrastructure, enabling localised Chinese operations as well as local production of cloud hardware, and increasing Türkiye's dependence on Chinese cloud services and data storage. As Türkiye's e-commerce and digital sectors expand, these dependencies deepen, with some major Turkish companies now building their entire digital infrastructure on Chinese clouds and storing their data in data centres operated by Chinese companies. Sino–Turkish partnerships in AI development further pave the way for key public institutions and state agencies to build their future digital infrastructure on the architecture of Chinese firms.

In the realm of smart cities and related technologies, Chinese engagement has evolved from participation in urban development projects to influencing the design of Türkiye's urban connectivity and security architecture. This includes not only supplying surveillance systems to public and commercial sectors and developing next-generation technologies with Turkish national research actors, enabling Chinese companies to integrate their systems into the Turkish surveillance infrastructure and entrench themselves in local innovation pipelines, but also transferring technology in defence and border-security fields. This incorporates Chinese hardware and software directly into Turkish security platforms, which is critical and sensitive digital infrastructure. The various cooperation initiatives, both directly related to smart-city technologies and in interrelated sectors, such as 5G infrastructure or cloud computing, suggest a firmly established Chinese foothold in this sector as well.

Chinese engagement across these sectors provides opportunities for Türkiye to enhance its capabilities in information technology, AI, and smart manufacturing. In addition, R&D cooperation alongside technology transfer deals could support long-term advancements and strengthen Türkiye's role as a regional technology hub, aligned with Ankara's broader geopolitical ambitions. However, there are also risks associated with China's foothold in Türkiye's digital ecosystem. While Türkiye's ties with China temper current threat perceptions, its NATO membership and possible future frictions with Beijing make these risks significant.

The risks include (1) infiltration, surveillance, or sabotage; (2) leakage of technology or other expertise to Chinese-controlled entities; as well as (3) creation or deepening of existing dependencies in critical sectors on Chinese suppliers for goods and services. This study's assessment of Chinese engagement reveals implications extending across all risk categories. Concerning infrastructure, for instance, the integration of Chinese companies' software and hardware management tools into Türkiye's telecom backbone could compromise data sovereignty. Similar integration in Türkiye's critical urban infrastructure through smart-city technologies gives rise to espionage risks, even in critical sectors such as border security. Chinese network equipment could come with hidden vulnerabilities or backdoors, enabling data interception and disruption of communications. The parallel growth of Türkiye's e-commerce and cloud sector, in both of which Chinese companies have a firm presence, signals long-term technical and operational dependencies. Similarly, the recruitment of Turkish technical experts in locally established Chinese companies' R&D centres, could leak local know-how, compromise technological sovereignty, and lead to talent drain.

Chinese penetration and foothold in Türkiye's digital ecosystem could raise trust and interoperability concerns in Brussels and Washington over potential cyber and espionage risks. Compromised alliance security would also imply compromised Swedish security. Bilaterally, following Sweden's NATO accession, there are ongoing efforts to enhance Swedish–Turkish defence coordination. The Chinese foothold in the aforementioned sensitive sectors could indirectly affect Swedish security and intelligence operations and pose both security and competitive challenges to Sweden's cautiously expanding business presence in Türkiye. The timing is sensitive, given Ankara's ambitions for an enhanced Turkish role in the European security architecture and Türkiye's considerable potential as a NATO ally amid deepening regional turmoil. ■

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm
Tel: +46 8 5550 3000
www.foi.se

This text is a summary of the FOI report, *China's Foothold in Türkiye's Digital Ecosystem,* FOI-R--5807--SE.
The entire report may be obtained from *www.foi.se* or via the following QR code: