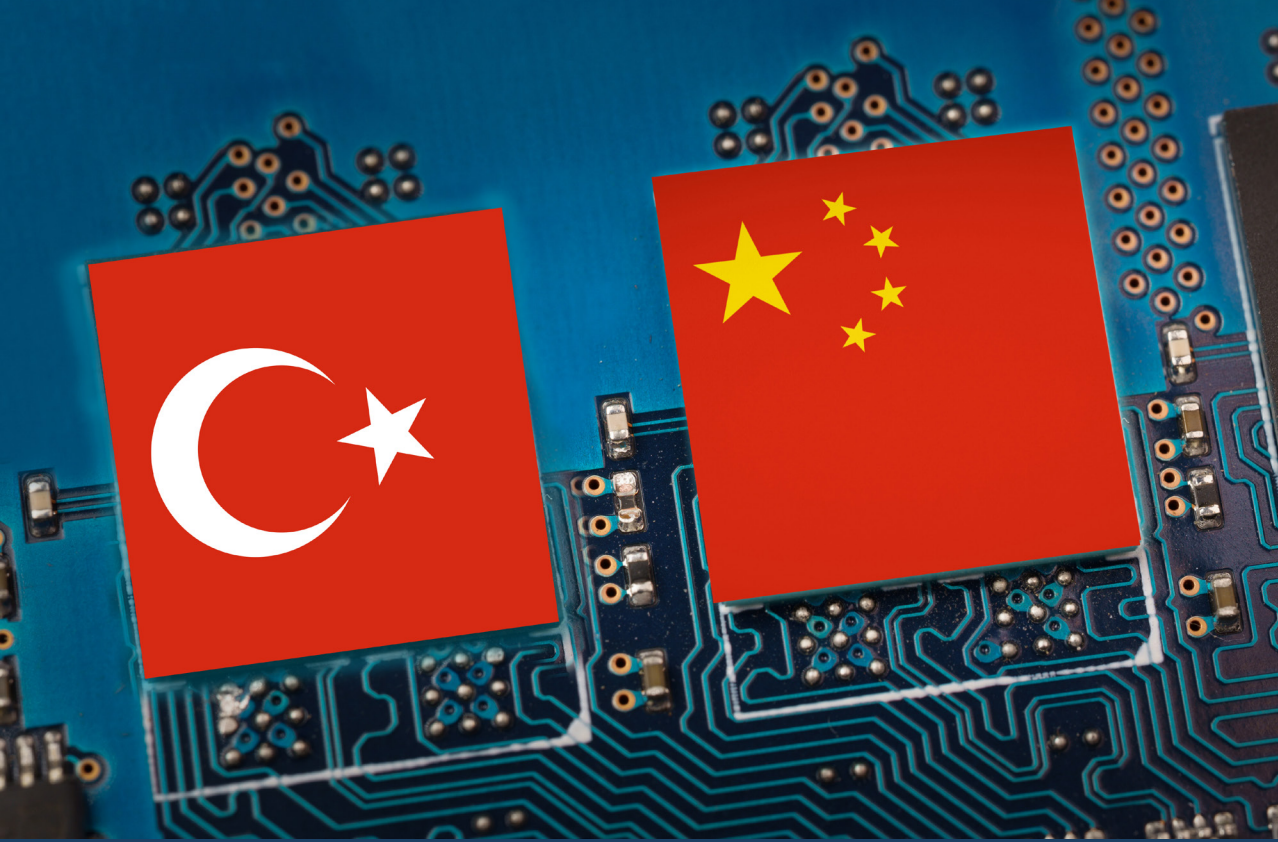

China’s Foothold in Türkiye’s Digital Ecosystem

Marianna Serveta

FOI-R--5807--SE

November 2025

FOI

Marianna Serveta

China’s Foothold in Türkiye's Digital Ecosystem

Title	China’s Foothold in Türkiye's Digital Ecosystem
Titel	Kinas fotfäste i Turkiets digitala ekosystem
Report no	FOI-R--5807--SE
Month	November
Year	2025
Pages	73
ISSN	1650-1942
Client	Ministry of Defence
Forskningsområde	Säkerhetspolitik
FoT-område	Inget FoT-område
Project no	A12504
Approved by	Daniel Faria
Ansvarig avdelning	Försvarsanalys

Cover: Shutterstock, edited by the Swedish Defence Research Agency

Sammanfattning

Denna studie undersöker omfattningen av kinesiska affärsengagemang i Turkiets digitala ekosystem. Resultatet visar ett betydande och mångfacetterat engagemang, i form av investeringar och samarbetsavtal, vilket gör det möjligt för Kina att etablera ett starkt fotfäste inom alla delområden som utgör ett digitalt ekosystem: telekommunikationsinfrastruktur, ekonomiska plattformar och finansteknologi, samt molntjänster och smarta stadsteknologier. Studien bygger på det teoretiska antagandet att kinesisk förankring i ett lands digitala ekosystem ger Peking fördelar som kan omsättas i politiskt tryck (eng. *weaponisation*). Därför reflekterar studien även över en rad risker kopplade till Kinas fotfäste i Turkiets informations- och digitala infrastruktur, både för Turkiet självt och för dess västerländska allierade, och i förlängningen för svenska intressen och säkerhet.

Nyckelord: Turkiet, Kina, Nato, digitala sidenvägen, cybersäkerhet, övervakning, digitalt ekosystem, telekom, e-handel, digital betalning, fintech, smarta städer, säkerhetsinformationssystem, molntjänster, datacenter, strategisk autonomi, investeringar, Sverige

Summary

This study explores the areas and extent of Chinese business engagement in Türkiye's digital ecosystem. It finds considerable and multi-layered engagement, in the form of investment and cooperation agreements, which have enabled China to establish a strong foothold across all areas that comprise a digital ecosystem: telecommunications infrastructure, economic platforms and financial technology, cloud computing and smart-city technologies. The study's underlying theoretical assumption is that Chinese entrenchment in a country's digital ecosystem gives Beijing leverage to engage in activities of weaponisation. Therefore, the study also reflects on a wide array of risks associated with China's foothold in Türkiye's information technology and digital infrastructure, both for Türkiye itself and for its Western allies, and, by extension, for Swedish interests and security.

Keywords: Türkiye, China, NATO, Digital Silk Road, cybersecurity, surveillance, digital ecosystem, telecom, e-commerce, digital pay, fintech, smart city, security information systems, cloud, data centres, strategic autonomy, investment, Sweden

Executive summary

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 purpose is to examine China's foothold in Türkiye's digital ecosystem. It also seeks to reflect on the risks associated with this foothold for Türkiye itself and for its Western allies. The 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 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, Research and Development (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.

Abbreviations

AI	Artificial Intelligence
AKP	*Adalet ve Kalkınma Partisi* (Justice and Development Party)
BRI	Belt and Road Initiative
BRICS+	Expanded format from original composition of Brazil, Russia, India, China, and South Africa; additional members vary by year
DEİK	Foreign Economic Relations Board of Türkiye (*Dıs Ekonomik¸ İli¸skiler Kurulu*)
DSR	Digital Silk Road
IoT	Internet of Things
ISAC	Integrated Sensing and Communication
ICT	Information and Communications Technology
MoU	Memorandum of Understanding
NATO	North Atlantic Treaty Organisation
POS	Point-of-sale
R&D	Research and Development
SIS	Security Information Systems
TCBM	Central Bank of the Republic of Türkiye (*Türkiye Cumhuriyet Merkez Bankası*)
TOBB	*Türkiye Odalar ve Borsalar Birliği*, Union of Chambers and Commodity Exchanges of Türkiye
TÜİK	Turkish Statistical Institute (*Türkiye İstatistik Kurumu*)
TÜSİAD	Turkish Industry and Business Association (*Türk Sanayicileri ve İş İnsanları Derneği*)

Table of contents

1 Introduction

NATO member Türkiye's relations with China have deepened in recent years. In 2010, the countries signed agreements elevating bilateral relations to the level of strategic cooperation.[1] This paved the way for enhanced diplomatic ties and military-technical collaboration. Ankara is seeking to bolster the country's economy by attracting foreign investment. China's investment in Türkiye has expanded significantly across multiple sectors, particularly automotive, infrastructure, and renewable energy. Tellingly, AVIC, one of China's largest state-owned defence-aerospace enterprises, invested USD 1.3 billion in Türkiye in 2019 to build a thermal power plant.[2] This means the heart of China's defence industry has gained a foothold in Türkiye's critical infrastructure.

China has shifted from primarily engineering, procurement, and construction to direct investment in Türkiye. In most areas, China's investment in Türkiye remains non-value-adding, meaning it has not yet translated into meaningful growth for Türkiye's economy.[3] Despite this, Türkiye encourages further Chinese investment and is deepening ties with a country that leading NATO actors see as a rival. This is part of Türkiye's pursuit of greater independence in its policy formulation and action, led by national interests rather than devotion to ideological or institutional constraints. In light of Türkiye's ongoing economic crisis, Beijing has become an important external lifeline for the Justice and Development Party (*Adalet ve Kalkınma Partisi*, AKP) and its cronies.[4] The advantages are mutual for Beijing. In a new era of escalating trade wars, Türkiye serves as both a production and distribution hub for Chinese companies, a logistics bridge to European, Middle Eastern, and African markets.

Türkiye's digital ecosystem has increasingly drawn China's attention lately. Türkiye's tech startup sector is one of the strongest in the Middle East and North Africa, second only to Israel's.[5] In recent years, multiple Chinese tech companies

[1] Colakoğlu, Selçuk (2018). "Turkey–China Relations: From strategic cooperation to strategic partnership," Middle East Institute, 20 March.
[2] *AEI* (2024). China Global Investment Tracker; *NS Energy* (2019). "Hunutlu Thermal Power Plant," 27 September.
[3] Value creation refers to an activity that produces outputs whose worth exceeds the cost of the inputs used. See, for instance, Mazzucato, Mariana, Shipman, Alan (2014). "Accounting for productive investment and value creation," *Industrial and Corporate Change*, Vol. 23(4), p. 1059–1085. Chinese value-added investments in Türkiye are concentrated in low-productivity and low-skilled sectors. See, for example, Gürel, Burak, Kozluca, Mina (2022). "Chinese investment in Turkey: The Belt and Road Initiative, rising expectations and ground realities," *European Review*, vol. 30 (6), p. 806–834.
[4] See for instance Nilgün, Eliküçük Yildirim, Gözde, Yilmaz (2023). "Use/misuse of Chinese BRI investment? BRI-related crony capitalism in Turkey," *Southern European and Black Sea Studies*, vol. 23 (2), p. 365–383.
[5] Mahfoud, Ayşe, Tecimer, Cem (2022). "The Turkish technology ecosystem: An introduction," *Norton Rose Fulbright*, 15 June.

have entered Türkiye's digital market. Türkiye has also set ambitious technological goals for the 21st century. Yet, because Türkiye is not among the global innovation leaders, it seeks international cooperation to realise its high-tech ambitions. On technology transfer, Ankara generally views China as a more cooperative partner than the US or European countries.[6]

Chinese tech companies' engagement in Türkiye's high-tech sector is not hindered by Türkiye's NATO membership. This is largely assisted by the fact that there is no consensus among NATO allies regarding key matters such as investment screening that are relevant for critical infrastructure resilience. Despite NATO's efforts to create uniform roadmaps and agendas, the alliance still lacks common protection standards, for example on emerging and disruptive technologies.[7] At the same time, technological ecosystems are deeply transnational. Therefore, Türkiye's incremental move towards China's technology ecosystem is likely to continue.[8]

Chinese investment and technology penetration in Türkiye's digital ecosystem are understudied yet highly relevant, given the potential costly risks to Türkiye and, indirectly, its allies. Risks include cyber-espionage, influence operations, and technology leakage to China-controlled entities, with significant implications for connectivity and cyber sovereignty. Sweden has implemented measures to safeguard its network technologies against Chinese influence. However, Swedish security and interests could be indirectly impacted if an ally permits Chinese entrenchment in its digital infrastructure, especially where Swedish companies also operate.

The expanding Chinese footprint in Western digital ecosystems raises concerns that Beijing may be using Chinese companies' global reach to re-wire the global digital architecture, from physical cables to code. Considering the strengthening of Sino-Turkish relations, it is timely to examine how deeply Chinese companies have penetrated Türkiye's digital ecosystem.

1.1 Aim and research question

The aim of this study is to examine China's foothold in Türkiye's digital ecosystem. Thus, the main research question underpinning this study is:

[6] Öngür, Çandaş (2025). *The US–China Tech war: Where does Turkey stand?.* SWP Comment, No 12. Centre for Applied Turkey Studies, p.4.
[7] Nouwens, Meia (2022). *NATO and China: Addressing new challenges.* CSDS Policy Brief, p. 1, 4.
[8] For more about the transnational nature of technological ecosystems and the cost of technological decoupling, see, for instance, Kleinhans, Jan-Peter, Rühlig, Tim (2024). "Introduction: Reverse dependencies on China," in Rühlig, Tim (2024). *Reverse dependency: Making Europe's digital technological strengths indispensable to China*. Digital Power China Report 3, German Council on Foreign Relations.

What are the areas and the extent of China's business engagement in Türkiye's digital ecosystem?

The study further considers the impact of China's penetration of Türkiye's information technology and digital infrastructure on Türkiye and its Western allies, and by extension on Sweden's security and interests. Accordingly, the subsequent research question examined is:

What risks are associated with China's foothold in Türkiye's digital ecosystem?

1.2 Operationalisations and delimitations

Mapping the integration of Chinese technologies across all levels of Türkiye's Information and Communications Technology (ICT) supply chains is complex and beyond the scope of this study. This study instead covers China's foothold in Türkiye's digital ecosystem, according to what the author interprets as the Digital Silk Road's (DSR) objectives and related projects (see Section 2.2).

Previous research does not provide a systematic breakdown of the entities that comprise a national digital ecosystem. Progress in digitalisation has been measured through various composite indicators, as the Digital Ecosystem Development Index by Katz and Callorda; the Digital Economy and Society Index by the European Commission; the Network Readiness Index by Dutta and Lanvin; the ICT Development Index by the UN Telecommunication Union and the Global Index of Digital Entrepreneurship by Autio et al.[9] Most indices developed so far focus on particular aspects, such as broadband penetration or economic performance, and include a limited number of indicators. More comprehensive indices, such as Katz and Callorda's, provide detailed, multifaceted assessments of national digital ecosystems and a valuable framework for analysing domestic digital maturity. While that index covers domestic pillars, such as household digitisation and digital competitive intensity, it does not provide a framework for capturing foreign investment or foreign presence. The DSR encompasses a broad spectrum of digital and infrastructural sectors: next-generation cellular networks; fibre-optic, terrestrial, and submarine cables; satellite systems; artificial intelligence; safety and smart-city technologies; cloud services; data centres; e-commerce; and over-the-top applications (delivering services directly over the internet) including

[9] Katz, Raul, Callorda, Fernando (2018). "Accelerating the development of Latin American digital ecosystem and implications for broadband policy," *Telecommunications Policy*, vol. 42 (9), p. 661–681; European Commission (2020). I-DESI 2020: How digital is Europe compared to other major world economies? 17 December; Dutta, Soumitra, Lanvin, Bruno (2022). *The Network Readiness Index 2022*. Portulans Institute; International Telecommunications Union (2024). *Measuring digital development: The ICT Development Index 2024*. ITU Publications; Autio, Erkko, Komlósi, Éva, Szerb, Laszlo, Tiszberger, Monika, Park, Donghyun, Jinjarak, Yothin (2024). "Digital entrepreneurship landscapes in developing Asia: Insights from the Global Index of Digital Entrepreneurship Systems (GIDES)," ADB Economics Working Paper Series, No. 720. Asian Development Bank.

financial services.[10] In order to answer the first research question and based on a review of previous research, the present study categorises the relevant sectors in two broad categories and defines Türkiye's digital ecosystem as consisting of a) infrastructure and the b) digital sector, which includes platforms, services, and relevant technologies.

The Chinese government formally launched the DSR in 2015. The material for this study was processed in summer–autumn 2025. Thus, this study covers the period 2015–2024 with a particular emphasis on 2023–2024 in order to draw some conclusions about China's current engagement within Türkiye's digital ecosystem.

This study uses the following terms extensively: penetration, presence, foothold, and influence. The terms are conceptualised here as existing on a scale. In this study, penetration refers to the act of intruding into the fabric of the ecosystem and entering the market. Presence denotes the existence of Chinese businesses in Türkiye's digital market, with a focus on current activity and operations, without necessarily having long-term ambitions to remain. Foothold refers to a firmly established business presence, with an ambition to remain and/or the capacity to shape the sector in which the business operates. Influence is the final step on the scale: a business presence that aims to affect sectors beyond its immediate area of operation or to shape the overall character or development of the market. The last step should be viewed in conjunction with this study's theoretical assumptions (see Section 1.3.3). A visualisation of the scale follows below:

Penetration → Presence → Foothold → Influence

A detailed tally of all Chinese investments in Türkiye's digital ecosystem would not, by itself, be a representative indicator of China's ambitions to expand influence in Türkiye's digital market. Large investment amounts do not necessarily reflect a deep or meaningful engagement in the local economy. For example, substantial financial flows may be concentrated in a few sectors with limited spillover effects, or they may represent passive investments without active participation or control. Conversely, smaller investments might be strategically significant, involving key industries or technologies that have outsized economic or political impact. Importantly, the initial investment amount fails to capture subsequent developments such as reinvestments, divestments, operational expansions, or shifts that often provide a more accurate reflection of the investor's long-term intentions and commitment. These dynamic changes can significantly alter the investor's role and influence in the host economy, making initial capital figures an incomplete measure of presence or impact.

[10] Triolo, Paul (2020). "The Digital Silk Road and the evolving role of Chinese technology companies," in Gordon, David, Nouwens Meia (2020). "The Digital Silk Road: China's Technological Rise and the Geopolitics of Cyberspace," *Adelphi Series*, vol. 60 (487–489), p. 69; Lagiewska, Magdalena (2024). "Legal aspects of the digital silk road: Trends and challenges," in Sahakyan, Mher (2024). *Routledge Handbook of Chinese and Eurasian International Relations*. London: Routledge, p. 407, 408.

Accordingly, this study analyses instead China's foothold in Türkiye's digital ecosystem by looking into key Chinese investments alongside cooperation agreements. Cooperation agreements are herein envisioned to give a complementary picture of long-term engagement ambitions. The present study thus examines investments and cooperation agreements as the channels of Chinese engagement in Türkiye's digital ecosystem, and thus as foothold indicators.

1.3 Theoretical framework

The next section reviews prior research and introduces the concept of strategic autonomy, contextualising how Türkiye justifies its growing engagement with China. The subsequent section outlines the theoretical foundations of the present study.

1.3.1 Previous research and the concept of strategic autonomy

Technology and information now sit at the core of geopolitical power struggles. The existing literature conceptualises China's global digital expansion primarily through the lens of a Sino–US dispute. Some usual concerns raised in this regard are state surveillance, digital authoritarianism, spatial expansion of China's digital sovereignty, as well as the illusion of partner countries' data sovereignty when cooperating with China.[11] Moreover, an evolving line of research looks into the globalisation or transnational character of the Chinese internet, factors that link Chinese internet giants to international investment banks and venture capital.[12] The notion of a nascent Chinese digital empire, rooted in the competitive Sino–US dyad, is challenged by a relatively recent surge in research that examines local agency in newly incorporated geographies of Chinese influence, such as the Global South.[13] The present study positions itself in this latter research field.

[11] See, for instance, Wright, Charity (2021). "China's digital colonization: Espionage and repression along the Digital Silk Road," *SAIS Review of International Affairs,* Vol. 41(2), p. 89–113; Makowska, Marta (2024). *China's digital authoritarianism vs EU technological sovereignty: The impact on Central and Eastern Europe.* Council on Foreign Relations; Cong, Wanshu (2024). "The Spatial Expansion of China's Digital Sovereignty: Extraterritoriality and Geopolitics" In Jiang Min, Belli Luca (2024). *Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance.* Cambridge: Cambridge University Press; Erie, Matthew, Streinz, Thomas (2021). "The Beijing effect: China's Digital Silk Road as transnational data governance," *New York University of International Law and Politics,* Vol. 54(1), p. 1–92.

[12] See Qiu, Jack, Linchuan, Yu, Peter, Oreglia, Elisa (2022). "A new approach to the geopolitics of Chinese internets". *Information, Communication & Society,* Vol. 25(16), p. 2335–2341 and, respectively, Jia, Lianrui, Winseck, Dwayne (2018). "The political economy of Chinese internet companies: Financialization, concentration, and capitalization," *International Communication Gazette,* Vol. 80(1), p. 30–59.

[13] See, for example, El Kadi, Tin Hinane (2025). *Local agency is shaping China's digital footprint in the Gulf.* Carnegie Endowment, 6 January.

The case of Türkiye is significant because, as a NATO member, the country is deeply integrated into the Western defence architecture. Despite that, it is actively seeking to deepen its ties with China, a country that NATO views as a rival and sometimes also as a threat.[14] Türkiye has a long history of data leaks and breaches. The country's cybersecurity framework is grounded in a set of laws and regulations that govern the protection of information systems and critical infrastructure. The cornerstone is the Law on Cybercrime (Law No. 5651), enacted in 2007, which defines cyber offences and outlines procedures for investigation and prosecution. It underpins Türkiye's approach to combating threats such as unauthorised access, data breaches, and cyber fraud. Secondary regulations further refine the legal framework.[15] Progressively, the country has developed a comprehensive cybersecurity strategy that also informs its Development Plans; the national strategic roadmaps guiding the country's economic and technological policy.[16] Moreover, in March 2025, a new cybersecurity law came into force with the view to strengthen the country's digital infrastructure and enhance the country's digital security.[17] Türkiye's increasingly mature cybersecurity environment suggests that, in general, Ankara views digital technologies as having security relevance and, therefore, as potential vulnerabilities.[18] Despite that, Türkiye opens its digital ecosystem to Chinese actors. This, in turn, indicates that Ankara does not view Chinese ownership of Turkish digital technologies as inherently threatening, instead relying on political ties with Beijing to prevent undesired conduct. Türkiye's willingness to engage with China should be understood within the framework of strategic autonomy.

Strategic autonomy is a concept that is predominantly used in a defence context, yet holds different meanings across countries and is adopted with varying degrees of formality by their institutions. Türkiye has not published a revised military doctrine or a defence white paper since the 1990s. However, the concept is increasingly referenced by state representatives and in policy papers from leading Turkish think tanks and research institutions.[19] Moreover, the effects of the

[14] See, for instance, Simon, Luis (2023). "NATO's China and Indo-Pacific conundrum," NATO Review, 22 November.

[15] For an overview of those, see for instance Generis Global (2024). Overview of Cybersecurity Regulations in Turkey.

[16] For an overview in English, see for instance Yazıcıoğlu, Bora, İslamoğlu-Bayer, Kübra, Savaş, Aslı, Özdabakoğlu, Yağmur (2025). *Cybersecurity 2025: Turkey: Law and Practice.* Chambers and Partners.

[17] The law has been strongly criticised by opposition politicians, human rights groups, and legal experts who warn that the law could enable broad surveillance and restrict freedom of speech. See, for instance, Geybullayeva, Arzu (2025). "In Turkey, a controversial law on cybersecurity is widely seen as yet another censorship tool," *Global Voices,* 27 March.

[18] This reflects a securitised perspective on digital technologies. For more on securitisation, see Balzacq, Thierry, Leonard, Sarah, Ruzicka, Jan (2015). "Securitization revisited: Theory and cases," *International Relations,* Vol. 30(4), p. 494–531 and Mügge, Daniel (2023). "The securitization of the EU's digital tech regulation," *Journal of European Public Policy,* Vol. 30(7), p. 1431–1446.

[19] See, for instance, Yeşiltaş, Murat (2020). "Deciphering Turkey's assertive military and defence strategy: Objectives, pillars and implications," *Insight Turkey,* Vol. 22(3), p. 89–114.

strategic autonomy concept become visible in various official Strategic Plans for the defence industry, shaping the direction of defence development in Türkiye.[20]

The concept of strategic autonomy has been developed in Türkiye in response to the country's belief that the West does not take its security policy concerns seriously and as an adaptation to an emerging multipolar world order.[21] For Türkiye, strategic autonomy means retaining the capacity to act independently in different areas of defence and security policy when deemed necessary. This firstly involves the ability to independently assess the country's threat landscape. Secondly, it entails sustaining advanced military capabilities that can be deployed to safeguard national interests. Among other things, this entails diversifying procurement channels and expanding the country's partner network. In the Turkish analysis, strategic autonomy does not conflict with collective defence nor with the country's obligations as a NATO member. Strategic autonomy is rather seen as framing the country's efforts to protect its interests, which enables Türkiye to deepen its ties with non-traditional allies and ends up acting as leverage, often increasing Türkiye's value for its traditional allies in the West.[22]

Thus, to reduce dependencies and expand its room for manoeuvre, Türkiye views China, the world's second-largest economy and a leader in pioneering technological initiatives and development projects, as a key future partner.

1.3.2 Theoretical foundations of the present study

This study's theoretical point of departure is that of weaponised interdependence. Farell and Newman address structural imbalances among states, arguing that asymmetric network structures enable some states to leverage or weaponise independent relationships to coerce others.[23] States controlling the key hubs of global networks for money, goods, and information are uniquely positioned to impose costs on others.[24] Farell and Newman argue further that in order for states to gain advantages, they rely on either the *panopticon* or the *chokepoint* effect of a network. The former entails advantaged states exploiting physical infrastructure and using their advantageous position to extract information about their adversaries. The latter entails advantaged states limiting or cutting adversaries off from

[20] See Serveta, Marianna (2024). *Chasing the Red Apple: Turkey's Quest for Strategic Autonomy.* FOI Memo 8568. Kista: Swedish Defence Research Agency (FOI).
[21] Serveta, Marianna (2025). *Turkiets säkerhetspolitiska färdriktning: Strategisk autonomi och stormaktsberoenden* [Türkiye's security policy direction: Strategic autonomy and great power dependencies]. FOI-R--5781--SE. Kista: Swedish Defence Research Agency (FOI), p. 40.
[22] The author has previously explored the concept of strategic autonomy with regard to Türkiye's defence industrial evolution and also with regard to the country's foreign-policy action. See Serveta, 2024 and Serveta, 2025, respectively.
[23] Farrell, Henry, Newman, Abraham (2019). "Weaponized interdependence: How global economic networks shape state coercion," *International Security,* Vol. 44(1), p. 45.
[24] Ibid, p. 46.

network flows.[25] In the digital domain, digital technologies and supporting infrastructure could be exploited in this regard.[26] Building backdoors in hardware or software is an example of both panopticon and chokepoint, as an advantaged state can use a backdoor to both monitor data flows and disturb a network, denying an adversary access.[27] Naturally, it would be extremely damaging for China-Türkiye relations (and for the companies involved) if backdoors were discovered.

The potential for China to weaponise relationships of technological dependence by leveraging its firms' footholds in Western networks is a major concern for Western actors. Building on the theoretical framework outlined above, this study assumes that the presence and engagement of Chinese firms within a country's digital domain enables Beijing to carry out activities of weaponisation, provided it has the interest to do so. The risks associated with this weaponisation can be drawn from the work of Theodore Moran and Lindsay Oldenski, whose work looked into the threats associated with Chinese direct investment in the US.[28] The researchers argue that perceived threats to national security fall into three categories. The first threat category is that a foreign acquisition of a company would enable the insertion of some capability for infiltration, surveillance, or sabotage. The second threat category is the leakage of technology or other expertise to a foreign-controlled entity, which could be used in a manner harmful for national interests. The third threat category is that the acquisition could make the host country for an investment dependent on a foreign-controlled supplier of goods or services that are critical for the country's economy.[29] This threat categorisation is relevant even when it comes to cooperation agreements, the present study's second channel of Chinese engagement with Türkiye's digital ecosystem.

1.4 Material and method

There is extensive literature that looks into the extent to which Chinese investment is state-directed or initiated by private companies' interests.[30] It is beyond this study's scope to analyse the level of state control over the companies mentioned. Instead, the study proceeds from the premise that Chinese companies cannot

[25] Ibid.
[26] See, for instance, Mügge, 2023.
[27] Brown, Scott (2024). "Beyond the great firewall: EU and US responses to the China challenge in the global digital economy," *Journal of European Integration*, Vol. 46(7), p. 1093.
[28] Moran, Theodore, Oldenski, Lindsay (2013). *Foreign direct investment in the United States: Benefits, suspicions and risks with special attention to FDI from China*. Peterson Institute for International Economics.
[29] Moran, Oldenski, 2013, p. 55.
[30] See, for example, Milhaupt, Curtis, Zheng, Wentong (2015). "Beyond Ownership: State Capitalism and the Chinese Firm," *Georgetown Law Journal*, Vol. 103, p 665–722; Pearson, Margaret, Rithmire, Meg, Tsai, Kellee (2021). "Party–state capitalism in China," *Current History*, p. 207–213; Milhaupt, Curtis, Lin, Lauren, Yu-Hsin (2023*). Can Chinese firms be truly private?*. CSIS, Big Data China, 7 February; Almén, Oscar, Carlsson, Hanna (2025). *The Chinese Communist Party's influence over businesses*. FOI-R--5695--SE. Kista: Swedish Defence Research Agency (FOI).

operate in China without complying with government directives.[31] This is further supported by the fact that the Chinese government can also prevent and punish bad investment behaviour. The study assumes thereby that, although the Chinese government might not necessarily initiate an investment or cooperation agreement, it can influence, guide, or benefit from such engagements in line with broader strategic goals.

Official reports and analyses on firms operating in Türkiye are mainly produced by the Union of Chambers and Commodity Exchanges of Türkiye (*Türkiye Odalar ve Borsalar Birliği*, TOBB), the body publishing information regarding the presence of foreign companies in the country. TOBB bases its reports on the registry of the Ministry of Industry and Technology (*Sanayi ve Teknoloji Bakanlığı*), where all companies investing in Türkiye are required to register. Türkiye's Investment Office Vice President stated during his speech at the second China International Supply Chain Expo that as of mid-2024, more than 1300 Chinese companies operate in Türkiye.[32] TOBB currently has no publicly available compilation of foreign-investor data, and its most recent compilation (2019) of Chinese-invested firms in Türkiye has also been taken offline. Thus, the author of the present study directly examined the registry of the Ministry of Industry and Technology, which should thus be seen as the present study's primary source.

Before the Ministry of Industry and Technology made its latest registry public at the end of summer 2025, the author of the present study had contacted Burak Gürel and Mina Kozluca, who, in 2022, published a study on Chinese investments in Türkiye, based on the TOBB report from 2019.[33] The aim in making this contact was to gain an indication of the approximate number and names of Chinese companies that were then registered as operating in sectors particularly relevant for Türkiye's digital ecosystem, in order to examine their areas of operation more closely. This would suffice, considering that the present study's aim is to survey the engagement of Chinese companies in Türkiye's digital ecosystem, rather than to map all engagement. Exceeding the author's expectations, Gürel and Kozluca kindly shared their entire dataset for use in the present study.[34] Their dataset was then used for verification purposes alongside the Ministry of Industry and Technology's registry, mainly as a complementary reference for data sorting and categorisation.

---

[31] Hemmings, John (2017). *Safeguarding our systems: Managing Chinese investment into the UK's digital and critical national infrastructure.* The Henry Jackson Society, p. 13.

[32] Presidency of the Republic of Türkiye, Investment and Finance Office (2024). "Türkiye and China Strengthen Historic Ties for Future Economic Growth at CISCE 2024," 28 November.

[33] Gürel, Burak, Kozluca, Mina (2022). "Chinese investment in Turkey: The Belt and Road Initiative, rising expectations and ground realities," *European Review*, Vol. 30(6), p. 806–834. After crosschecking the data from the TOBB 2019 report, Burak Gürel and Mina Kozluca verified in their study that from those 1075, only 1004 firms were active (see Gürel, Kozluca 2022, p. 818).

[34] 4 July 2025, via email correspondence.

After examining the Ministry's registry, and in line with the statement made by Türkiye's Investment Office Vice President, this study assesses that 1419 Chinese companies were registered in Türkiye as of the end of June 2025.[35] This regards the companies listed under China in the Ministry's registry and not Chinese companies operating for instance from Singapore and thus listed under that country. Naturally, this could imply a significant amount of unreported data. Examining Chinese investments in Türkiye made through intermediary jurisdictions was considered to be beyond the scope of the present study.

The Ministry's registry initially classified the 1419 companies across 48 sectors. Sectors such as "Computer and related activities" or "Post and telecommunications" became immediately relevant for the present study's inquiry. However, after randomly examining such seemingly less relevant or irrelevant sectors as, for instance, "Electricity, gas, steam and hot water supply," it was noticed that companies relevant for the study's inquiry were also sorted there. An example is Yisun Elektronik ve Güvenlik Sistemleri Sanayi Ticaret Limited Şirketi, which, although listed under "Electricity, gas, steam and hot water supply," is active within the telecommunications (telecom) sector; it trades electronic devices and parts; imports, exports, and assembles security systems, recording devices, security cameras, and detection systems; as well as produces and maintains smart home technology. It is important to note that, nowadays, there is a significant overlap between modern energy solutions and digital technologies, such as smart grids. The particular example of misclassification could be due to this reason. This study does not examine the energy sector and therefore has neither included companies active there, nor verified whether their reported activity is relevant for the digital ecosystem.

The operations areas of all registered companies were verified online. Many of the companies operate in multiple sectors, as noticed both in the Ministry's registry and through the online verification. Those were therefore classified according to their primary operation as noted in the Ministry's registry. Where misclassifications were found, companies were re-categorised based on their own online descriptions of activity.

A problematic aspect of the Ministry's registry is that it does not note whether an investor is currently active in the country, failing thereby to monitor current operations and activity status. This could have been the reason behind some misclassifications. Indeed, during this cross-examination stage, not all registered companies were found to be active. Thus, in accordance with previous research, the active companies from the Ministry's registry were regrouped into five

[35] T.C. Sanayi ve Teknoloji Bakanlığı. Yabancı Sermayeli Firma Listesi. 30.06.2025 Tarihi itibariyle Türkiye'de faaliyette bulunan yabancı sermayeli firmalar listesi [Republic of Türkiye Ministry of Industry and Technology. List of companies with foreign capital in Turkiye as of the end of June 2025].

sectors.[36] Of the 1419 Chinese companies registered, 140 were found to be currently operating in areas relevant to Türkiye's digital ecosystem, with relevance assessed according to the author's interpretation of the DSR's objectives.

However, the Ministry's registry was not found to be exhaustive. There are Chinese companies based in China with publicly known investment and business activity in Türkiye, such as Dahua, which are not included in the registry. Therefore, the present study proceeded with tracking announcements, infrastructure rollouts, investment footprints, and cooperation agreements through open sources in English and in Turkish. Thus, the collection of the main companies as listed by the Ministry of Industry and Technology informed yet did not limit this study's effort to identify Chinese companies active in the sector in question. This tracking process also allowed moving further than only clarifying the main areas of operation and documenting penetration, to exploring the depth of Chinese engagement with Türkiye's digital ecosystem. Two public datasets further assisted the tracking of Chinese engagement. First was the IISS China Connects dataset, which consists of both officially labelled DSR projects and projects not officially labelled as part of the Belt and Road Initiative (BRI). The dataset includes projects undertaken by Chinese stakeholders in response to China's global infrastructure campaigns, but that have not received explicit endorsement from Beijing. Last updated in autumn 2022, this dataset is treated here as complementary, rather than central. Second is the American Enterprise Institute's Chinese Investment Tracker. This dataset only records investments over USD 100 million, making it an insufficient, yet still useful, source for identifying the most ambitious signs of Chinese engagement in the Turkish digital ecosystem in terms of initial investment. Similar to IISS's dataset, this dataset was also seen as a complementary source.

To track additional Chinese engagement, including smaller investments and cooperation agreements, reports, articles, and media content were reviewed manually and with assistance from the Artificial Intelligence (AI) tool ChatGPT. As already noted, TOBB currently has no publicly accessible compilation of data on foreign investors. TOBB's monthly bulletins of established and closed firms for the years 2015–2024 were used as background material and as a complementary verification source for the present study. The Central Bank of the Republic of Türkiye (*Türkiye Cumhuriyet Merkez Bankası*, TCBM), the Foreign Economic Relations Board of Türkiye (*Dıs Ekonomik, İli¸skiler Kurulu*, DEİK) and the Turkish Statistical Institute (*Türkiye İstatistik Kurumu*, TÜİK) compile general data on the Turkish economy. These actors' annual statistical reports also formed part of this study's background material.

From this tracking process, an additional 11 Chinese companies were identified, beyond the 140 verified in the Ministry of Industry and Technology's registry. One

[36] For classifications, see, for instance, Gürel, Kozluca 2022; Camba, Alvin (2020). "The Sino-centric capital export regime: State-backed and flexible capital in the Philippines," *Development and Change,* Vol. 51(4), p. 970–997.

methodological limitation is that Chinese-language sources on outbound investment could not be examined, potentially omitting relevant information due to language barriers. Even if research in Chinese had been possible, though, it is not guaranteed that these sources would provide a more complete picture of Chinese outbound investments, as China's Ministry of Commerce, for instance, does not report investments routed through intermediary jurisdictions. Another limitation is that many actors do not publicly disclose their activities. Furthermore, investments often occur through subsidiaries or indirect channels, making it difficult to capture them in media coverage. All these limitations explain why the study cannot claim to have comprehensively mapped Chinese business activity. The study's ambition, however, was to identify the areas in which Chinese companies operate within Türkiye's digital ecosystem. Therefore, the limitations were deemed acceptable. The sectoral distribution of the 151 (140 + 11) Chinese companies identified by this study is summarised in Table 2 in the first section of Chapter 3.

Based on the list of technologies at the core of DSR, this study listed investments and cooperation agreements under two broad categories: a) infrastructure and the b) the digital sector. Infrastructure refers to the physical components of a digital ecosystem. This infrastructure forms the foundation that enables digital services, connectivity, and technological development across sectors. The digital sector refers to the services and technologies involved in producing, maintaining, and delivering digital goods essential for communication, data processing, and innovation. After processing the material, the following subunits emerged:

Infrastructure
- Telecommunications

Digital sector
- Economic platforms and financial technology
- Cloud computing
- Smart city technologies

In the infrastructure sector, telecommunications refer to the process of transmitting information over a distance, by means of cables or wireless signals.

In the digital sector, the first subunit deals with e-commerce, digital pay systems, and financial technology (fintech). E-commerce is the purchase or sale of goods between businesses, households, individuals, governments, and other public and private organisations over computer networks and the internet. For payments to be facilitated, the exchange of data is required.[37] A digital pay system is a method of electronically transferring money, using devices such as smartphones, computers, or payment cards, enabling secure cashless transactions. Fintech refers to the use

[37] Aydın, Erdal, Kılınç, Savrul, Burcu (2014). "The relationship between globalization and e-commerce: Turkish case," *Procedia—Social and Behavioural Sciences,* Vol. 150, p. 1268, 1269.

of digital technology to deliver financial services efficiently and innovatively, often through platforms, apps, or automated systems.[38]

The second subunit involves cloud computing and data centres. The cloud refers to on-demand computing services (e.g., storage and processing) delivered over the internet. Data centres are the physical facilities (e.g., servers, power and cooling, and networking equipment) that underpin those cloud services.[39]

The third subunit refers to smart cities and related technologies. "Smart" cities use technology-based solutions to improve the quality and performance of urban services, with a view to managing key assets, resources, and overall costs efficiently.[40] Smart cities are built on infrastructure that relies on ICT and sensor networks, aiming to enhance urban connectivity by improving public engagement and streamlining government operations.[41] Security information systems (SIS), which are relevant to smart cities, are integrated digital systems for monitoring, threat detection, and security management.

It is essential to note that all these subunits, both within a sector and across sectors, are interrelated. For instance, smart cities store data, which requires cloud services. Similarly, network technologies are vital for smart cities to function, just as infrastructure and its maintenance are necessary for SIS to operate.

1.5 Disposition

The present introductory chapter is followed by a background chapter, which first provides an overview of Sino-Turkish relations, and then introduces the DSR and Türkiye's involvement in the initiative. Chapter 3 presents the empirical findings. It first presents the sectoral distribution of the companies found to be active in Türkiye's digital ecosystem. It then details key investments and cooperation agreements across the subunits identified above, together with an analysis of their implications for China's foothold in Türkiye's digital ecosystem. The chapter ends by summarising the findings. Chapter 4 explores the risks associated with China's foothold in Türkiye's digital ecosystem, for Türkiye and its Western allies. The chapter then considers the consequences for Swedish interests and security. Chapter 5 offers suggestions for future research, based on both the present study's delimitations and its findings.

---

[38] See, for instance, Gomber, Peter, Koch, Jascha-Alexander, Siering, Michael (2017). "Digital finance and FinTech: current research and future research directions," *Journal of Business Economics*, Vol. 87, p. 537–580.

[39] See, for example, *MSoftserv* (2025). "Difference between cloud computing and data centre?" 19 June.

[40] See, for instance, Caragliu, Andrea, Del Bo, Chiara, Nijkamp, Peter (2011). "Smart cities in Europe," *Journal of Urban Technology*, Vol. 18(2), p. 65–82.

[41] Ismagilova, Elvira, Hughes, Laurie, Rana, Nripendra, Dwivendi, Yogesh (2022). "Security, privacy and risks within Smart Cities: Literature review and development of a Smart City interaction framework," *Information Systems Frontier*, Vol. 24, p. 393–414.

2 Background

This chapter provides the context for understanding the current deepening of Türkiye–China relations on the digital front. Section 2.1 offers a brief historical overview of the bilateral relations, covering political, defence, and economic ties. Section 2.2 provides an overview of the DSR concept, and Türkiye's incorporation into the DSR initiative. Readers who wish to go straight to the study's empirical findings may proceed to Chapters 3 and 4.

2.1 Overview of Sino–Turkish relations

Türkiye and China share a long history of interaction, dating back to the Silk Road era when trade and cultural exchange flourished. During some periods, the interaction was violent, as various Turkic nomadic tribes and states waged war against Chinese expansion in Central Asia. During the Ottoman period, direct relations between China and the Ottoman Empire were minimal.

In Türkiye's modern history, after the formation of the Turkish Republic in 1923, Türkiye–China relations have been shaped by ideological rivalry. With the easing of tensions between China and the US, Türkiye's foremost ideological ally, in the early 1970s, and as a result of episodic crises between Türkiye and the West, Türkiye established formal diplomatic ties with China in 1971. During the 1980s, economic ties flourished and diplomatic exchanges accelerated.[42] However, multiple crises regarding the Uyghur issue and Türkiye's Xinjiang policy strained the countries' relations during the 1990s.[43] Türkiye, which shares ethnic, religious and cultural ties with the Uyghurs, has historically expressed concern over their treatment in China's Xinjiang region. China, for its part, frames its actions in Xinjiang as counter-terrorism and internal security measures.[44] The emergence of Kurdish separatism in Türkiye in the 1990s helped persuade the Turkish political establishment to view China's challenges in Xinjiang as a domestic issue, and as comparable to Türkiye's own issues with the Kurds.[45]

Not even during those times when relations were strained, however, did the economic and military bonds between the two countries break entirely. The West's refusal to sell arms to Türkiye due to its human rights violations during its conflict

[42] See for instance Özşahin, Mustafa, Donelli, Federico, Gasco, Riccardo (2021). "China–Turkey Relations from the perspective of neoclassical realism," *Contemporary Review of the Middle East*, Vol. 9(2), p. 218–239.

[43] Çolakoğlu, Selçuk (2012). "Turkey's East Asian Policy: From security concerns to trade partnerships," *Perceptions*, Vol. 17(4), p. 129–158.

[44] For more on the Uyghur issue, see, for example, Yıldırım, Nılgün (2024). *The Uyghur issue in Turkey–China relations.* Heinrich Böll Stiftung, 5 April.

[45] For an account of how China uses the Kurdish issue in a tit-for-tat with Turkey, see, for instance, Akcay, Nurettin (2021). "Amid tensions with Turkey, China is putting the Kurdish issue in play," *The Diplomat*, 4 December.

with the PKK led Türkiye to seek alternative supporters for its defence-industrial efforts from the second half of the 1990s. Ankara's opening to Beijing for this purpose led to, among other things, a military cooperation agreement in 1996 for joint production of a short-range, ground-to-ground missile system.[46]

2.1.1 The AKP in power

The Sino-Turkish relations regained momentum when the AKP came to power in Türkiye in the early 2000s. Türkiye's renewed status as an "emerging regional power" attracted China's interest, as it was itself a rising economy. Beijing was also looking to build cooperative relations with regional actors in its efforts to soft-balance the US in the Middle East.[47] The AKP government in Türkiye then undertook various initiatives aimed at diversifying the country's political and economic relations and thereby claim a new role in the international system. Tellingly, Chinese companies took part in major infrastructure projects in the 2000s and China became Türkiye's third-largest trade partner by 2008.[48] Even in the defence industry, Türkiye's updated defence procurement policy, introduced in 2003, replaced licenced and joint production with an indigenous development model. Among other benefits for local capacity building, this updated policy broadened the country's potential for international cooperation and paved the way to build stronger defence ties with countries like China.[49]

2.1.2 Bilateral relations elevated to strategic partnership

Following the signing of a joint communiqué in 2010, Sino–Turkish relations were elevated to a strategic partnership.[50] The main aims of the partnership were to overcome political problems in bilateral relations, deepen economic ties, and develop a Sino–Turkish common global vision.[51] Although developing a common vision has been largely unsuccessful, both countries have made efforts since then to avoid tensions and have developed a mutual trust mechanism for preventing crises that may arise from their conflicting views on the Xinjiang and the Taiwan issue.[52]

---

[46] *Millitet* (1996). "Çinle gizli füze anlaşması" [Secret missile deal with China], 20 December; Weitz, Richard (2010). "Turkey and China establish strategic partnership," *The Turkey Analyst*, 25 October.
[47] Özşahin, Donelli, Gasco 2021, p. 11.
[48] Çolakoğlu, Selçuk (2015). "Dynamics of Sino–Turkish relations: A Turkish perspective," *East Asia*, Vol. 32, p. 21.
[49] See, for instance, Serveta, 2024; Egeli, Sıtkı (2019). "Making sense of Turkey's Air and Missile Defense Merry-go-round," *All Azimuth*, Vol. 8(1), p. 69–92.
[50] Osmanlı, Seyda Nur (2024). "Türkiye-Çin İlişkileri: İmkanlar ve zorluklar" [Turkey–China relations: Opportunities and challenges], *Center for Eurasian Studies*, Vol. 19, 22 November.
[51] Çolakoğlu, Selçuk (2013). "Sino-Turkish Relations: Assessments & Shortcomings," *China Policy Institute*, 1 October.
[52] For Turkey's view on the Taiwan issue, see, for instance, Çolakoğlu, Şelcuk (2021). *Turkey's Policy towards Taiwan: From Cross-Strait Relations to Syrian Refugees.* Global Taiwan Institute, 13 January.

The establishment of the strategic partnership was followed by a joint aerial exercise the same year, marking the first time a NATO country's air force conducted a drill with China's. After that, Türkiye and China have progressively strengthened their military cooperation.[53] A concrete result of the strengthened cooperation on the military-technological front is the short-range ballistic missiles J-600T Yıldırım and Bora, developed from the Chinese model B-611 and produced by the Turkish company Roketsan. These missiles have been incorporated into the Turkish Armed Forces' arsenal since 2001 and 2018, respectively.[54] That the military-technological cooperation has borne fruit contributes to both sides remaining committed to continuous joint efforts.

The continuous commitment to cooperation stems also largely from Ankara's appreciation of Beijing's technology-transfer policy. This was evident in many cases, for instance in 2013, when a Chinese company won Türkiye's tender to purchase the FD-2000, an air and missile defence system, thanks not only to its low price but also to its favourable technology-transfer policy.[55] Later on, the initiative was anticipated to advance into a joint development of Türkiye's own long-range air-defence capabilities. The whole initiative ultimately failed, however, largely due to NATO objections.[56]

2.1.3 The strategic partnership's economic dimension

The Sino–Turkish strategic partnership is mostly visible in the context of economic relations. To a large extent, this is because the strategic partnership almost coincided with the third electoral victory of the AKP in 2011, after which the country's political economy started shifting from a social and regulatory neoliberal model to an increasingly hybrid model of authoritarian capitalism, similar to that of Beijing.[57] The earlier periods of growing trade were followed by more comprehensive economic cooperation between China and Türkiye in the second decade of the 2000s. This concerned not only trade, which in itself grew in volume from USD 1.6 billion in 2003 to USD 27.27 billion in 2015 and USD 48 billion in 2023, but also tighter cooperation across various sectors, including investment, energy, and infrastructure.

---

[53] Alemdaroğlu, Ayça, Tepe, Sultan (2023). "Turkey's strategic partneship with China: A feminist recount" In Özkeçeçi-Taner, Binnur, Açıkmeşe, Sinem (2023). *One hundred years of Turkish foreign policy (1923–2023): Historical and theoretical reflections*. Cham: Palgrave MacMillan, p. 194.

[54] Kasapoğlu, Can (2019). "Türkiye'nin balistik füze teknolojisinde yeni aşama" [A new step in Turkey's ballistic missile technology], *Anadolu Ajancı*, 26 June.

[55] Egeli, Sıtkı (2019). "Making sense of Turkey's Air and Missile Defense Merry-go-round," *All Azimuth,* Vol. 8(1), p. 74; Also see the interview of Cansu Çamlıbel with Murad Bayar, Türkiye's head of the Undersecretariat for Defense Industries at the time; Çamlıbel, Cansu (2014). "Turkey 'cannot ignore' Western concerns over missile deal," *Hürriyet English*, 18 February.

[56] Egeli, 2019, p. 69–92.

[57] The latter model gained prominence particularly after the shift to the presidential system in 2018; see Uluyol, Yalkun (2024). *Partnership with limits: China Turkey relations in the late AKP era*. Heinrich Böll Stiftung, 20 March.

In 2013, China launched BRI an economic and infrastructure project aimed at improving infrastructure, trade routes, and connectivity across Asia, Europe, and Africa. Although Türkiye had received BRI-related investments since the initiative's inception, the country officially became a BRI member in 2015.[58] Chinese BRI-related investments in Türkiye have spanned various sectors, including energy, infrastructure, and technology. The Ankara-Istanbul High-Speed railway line, the 1915 Çanakkale Bridge, which connects the two sides of the Dardanelles Strait, the China Sunergy CSUN solar power facility, and the GK-2 Earth observation satellite are some examples of such investments and tighter Sino–Turkish cooperation.[59] Among the most comprehensive Turkish contributions to the BRI is the Baku–Tbilisi–Kars railway, which connects Türkiye to Georgia, Azerbaijan, and, by extension, China. Another example is the sale of a 65% stake in Türkiye's third-largest port, Kumport in Istanbul, to a Chinese consortium led by the state-owned company COSCO.[60]

Beyond the direct project-based outcomes, a country's involvement with the BRI has broader economic implications. Among these are engagement with Chinese state-owned enterprises and the provision of credit from development banks.[61] Indeed, since 2016 Türkiye has been the second-largest recipient, after India, of loans from the Asia Infrastructure and Investment Bank, which China sees as a competitor of the World Bank.[62] The various projects that Türkiye and China cooperate on have necessitated financial integration and economic policy coordination between the countries. Türkiye's expressed interest in joining the Shanghai Cooperation Organisation and BRICS+ further highlights Ankara's willingness to deepen its economic ties with Beijing at all levels.[63]

Türkiye's economic exchanges with China have also contributed to the AKP's survival in power. In recent years, the central bank has relied more heavily on currency swaps. This is because it has drained its foreign reserves by selling hard currency through public banks in an effort to stabilize the struggling Turkish lira and control exchange rates, elements that are vital for Türkiye's import-dependent

[58] China and Turkey signed the "Memorandum of Understanding on Aligning the Belt and Road Initiative and the Middle Corridor Initiative" in November 2015, during the G-20 Summit in Antalya; see Presidency of the Republic of Türkiye, Ministry of Foreign Affairs. Türkiye's Multilateral Transportation Policy.

[59] Hussain, Ejaz (2022). "The Belt and Road Initiative, the Middle Corridor and Turkey's Asia Policy: An Analysis," in Anas, Omair (2022). *Turkey's Asia Relations.* London: Palgrave Macmillan, p. 218.

[60] Presidency of the Republic of Türkiye, Investment Office (2015). "Chinese consortium buys into Turkish port with USD 940 million investment," 28 September.

[61] Du, Julan, Zhang, Yifei (2018). "Does one Belt one Road Initiative promote Chinese overseas direct investment?" *China Economic Review*, Vol. 47, p. 189–205.

[62] Uluyol, 2024.

[63] *BBC News Türkçe* (2022). "Erdoğan: Hedef Şanghay İşbirliği Örgütü üyeliği" [Erdoğan: The goal is membership in Shanghai Cooperation Organisation], 17 September; Hacaoğlu, Selcan, Kozok, Firat (2024). "Turkey Bids to Join BRICS in Push to Build Alliances Beyond West," *Bloomberg*, 2 September.

economy.[64] The amount of Türkiye's bilateral trade with China conducted in yuan instead of the US dollar has increased in value from USD 1.6 billion in 2012, when the first swap deal was signed, to USD 6 billion in 2021 after the swap deal was renewed.[65] The cash flow this has triggered has both set the country's economy in motion and boosted the central bank's reserves.[66] The flow of cash has also facilitated the AKP's clientelistic practices ahead of elections. This concerns the contracts that the government assigns directly to the patronage networks built and maintained during the AKP's two decades of continuous rule. In return, these business people and their extended networks help re-elect Erdoğan with their votes, donations, and public diplomacy.[67] The currency swap agreement was renewed in June 2025.[68]

2.1.4 Trade and investment

Trade between the countries is on the rise, and Türkiye is dependent on Chinese imports. In 2024, China ranked as Türkiye's top import partner, accounting for 13% of the country's total imports. Conversely, Türkiye's share of China's total imports generally hovers around 1–2%.[69] The overall trade relationship between Türkiye and China is heavily imbalanced, with China being the primary contributor to Türkiye's trade deficit. In 2023, the Sino–Turkish trade volume reached USD 43.4 billion, however, China's exports to Türkiye amounted to USD 39.07 billion, while Türkiye's exports to China amounted to USD 4.33 billion.[70] Apart from the volume, the Sino–Turkish trade relationship is also imbalanced in terms of substance. Türkiye's imports from China consist largely of components and goods that are vital for local industry, such as machinery, electrical components, and iron. The country's exports to China, by contrast, consist mainly of mineral products and materials that have low value for the Turkish economy.[71]

Chinese investment in Türkiye has expanded significantly, mainly in the automotive, infrastructure, and energy sectors. A recent example of a large initial investment in the Turkish energy sector is the Chinese Ganfeng Lithium Group's

[64] Sönmez, Mustafa (2022). "Turkey's central bank continues window dressing with currency swaps," *Al Monitor,* 26 June.
[65] Ibid.
[66] This refers to the heading gross reserves and not to hard currency reserve.
[67] Terihoğlu, Merve (2022*). Cronies in crises: Economic woes, Clientelism, and elections in Turkey.* Heinrich Böll Stiftung; Esen, Berk, Gumuscu, Sebnem (2020). "Why did Turkish democracy collapse? A political economy account of AKP's authoritarianism," *Party Politics,* Vol. 27(6), p. 1075–1091.
[68] Türkiye Cumhuriyet Merkez Bankası (2025). "Central Bank of the Republic of Turkiye and People's Bank of China renew bilateral currency swap arrangement," 13 June.
[69] OEC (2025). China Trade Data. The 1–2% is low compared to other European countries. For example, Germany accounted for approximately 7.3 %, and the Netherlands for around 3.5% of China's total imports in 2024. Türkiye's share is closer to that of France, which accounted for about 1.6% in the same year. See Destatis (2024). Press release No. 193 of 17 May 2024; Interesse, Giulia (2024). "China's export surge: A closer look at H1 2024 Trade Expansion," *China Briefing,* 30 July.
[70] Xiao, Estelle (2024). "China–Türkiye trade and investment profile," *ChinaBriefing,* 18 October.
[71] International Trade Centre. Bilateral trade between China and Türkiye in 2024. Product: All products.

investment of USD 500 million in autumn 2024 for the production of lithium batteries.[72] The need for energy use is likely to increase in the future with the growth of data centres and AI. This is because data centres require significant power for storage, processing, and cooling, while AI systems demand substantial processing power, memory, and storage capacity, which further drives energy consumption. Thus, similar investments in this sector should be expected to grow in parallel with cooperation agreements between Turkish and Chinese companies.[73] An example of such a cooperation agreement is the one made in 2024 between the Turkish company IBT Solar and the world's largest battery manufacturer, the Chinese firm CATL, for deepening collaboration in energy storage and developing battery products.[74]

The sectors where Chinese investments in Türkiye are on the rise are generally considered value-added sectors. However, at present, Chinese investment in Türkiye has only partially benefited low-productivity sectors, which do not drive the capability potential of the Turkish industry. This is consistent with Türkiye's existing trade deficit with China. The Turkish market is still dominated by European companies. However, considering that recent Chinese investments in Türkiye entail local production, this has the potential to change in the future.[75]

Sustaining and deepening the Sino-Turkish partnership

Türkiye has ambitious geopolitical goals, both regionally and globally, which include, among other things, the desire to ensure strategic dominance in relation to regional crises, to project its power in established and new geographies, and to become a decisive pole in reforming the international system.[76] Its various goals

[72] President of the Republic of Türkiye. Investment and Finance Office (2024). "Ganfeng Lithium and Yiğit Akü Announce USD 500 Million Battery Investment in Türkiye," 5 September.

[73] *Türkiye Gazetesi* (2025). "1 milyar dolarlık hamle! Tarifeler korkuttu, yatırımı öne çektiler" [A 1 billion dollar move! Tariffs caused concern, so they brought the investment forward], 2 July.

[74] *Dünya* (2024). "IBT Solar dünyanın 1 numaralı batarya üreticisi CATL ile işbirliği yapıyor" [IBT Solar Collaborates with the World's Number One Battery Manufacturer CATL], 27 May.

[75] An example of an investment that includes local production is the USD 1 billion investment made in 2024 by the Chinese electric-vehicle giant BYD. Although the initial investment may not be especially large, this kind of investment is expected to bear fruit in the long run, because opening production facilities in Türkiye will boost local manufacturing capabilities. It will also likely have spillover effects, since it opens the door for more Chinese automotive companies to invest in Türkiye. However, it will likely increase Türkiye's dependence on China for lithium batteries, which are strategic products in today's economies and especially in the tech sector. See, for instance, He, Laura (2024). "Chinese EV giant BYD to build $1 billion plant in Turkey," *CNN*, 9 July; Atlı, Altay (2024). "Çin'in Türkiye'ye dev yatırımı hangi kapıları açabilir?" [What doors could China's massive investment in Turkey open?], *Fikir Turu*, 6 August. Signs of efforts to boost local battery production are already visible, for instance through the establishment of Sino, a battery company formed through the partnership between the Turkish electric-car manufacturer Togg and the Chinese-government-controlled lithium company Farasis Energy, which produces battery modules and packs for smart devices. However, it is questionable whether such efforts can meet the massive energy demands that will be required by both the automotive and the infrastructure sectors, potentially indicating growing future dependencies instead.

[76] See Serveta, 2025, p. 23–33.

necessitate a stabilised economy, as well as advanced military, industrial, and technological capabilities. On the other hand, China has an interest in expanding its economic influence, in strengthening regional connectivity, and in projecting soft power. Within this framework, the Sino–Turkish partnership can be expected to endure and potentially deepen further. Indeed, the second meeting of the Türkiye–China Intergovernmental Cooperation Committee, held in November 2024, which is the highest-level consultation mechanism between the two countries, reaffirmed the countries' ties. At the meeting, the Turkish Minister of Treasury and Finance stated Türkiye's intention to strengthen cooperation with China in, among other areas, digital transformation, while the Chinese Vice Premier highlighted the countries' common interests in the area, among others, of 5G technology. During the meeting, the parties announced the establishment of a joint working group, to further align Türkiye and China's initiatives in areas relevant to the BRI.[77]

2.2 Digital Silk Road

At the heart of the general concerns regarding the rise of the Chinese digital sector is the possibility that the Chinese government uses Chinese companies and their global outreach to "rewire the global digital architecture from physical cables to code."[78] Naturally, that would have large implications for global connectivity, cyber freedom, and cyber sovereignty.[79]

Unlike the BRI, which the Chinese government extensively describes in official documents, it is less clear what the DSR entails. The Chinese government formally launched the DSR in 2015 with the intention of developing the advanced technological aspects of BRI and focusing on enhancing global digital connectivity. The DSR's initial defining characteristics emphasised hard-wired aspects of communication technology.[80] While, initially, official documents only referred to the cyber domain in the context of fighting and preventing cybercrime, by 2017 the DSR had entered the Chinese Communist Party's doctrine and became a central aspect of the BRI strategy. At the Belt and Road Forum in 2019, it was named as an initiative in its own right.[81] The following year, the DSR became a

[77] Presidency of the Republic of Türkiye. "Türkiye's FDI Landscape at a glance 2024," p. 322.
[78] Gordon, Meia, 2020, p. 16.
[79] China understands the principle of cyber sovereignty in terms of greater state control along with the governance of the internet; see Lagiewska, Magdalena (2024). "Legal aspects of the Digital Silk Road: Trends and Challenges" in Sahakyan, Mher (2024). *Routledge Handbook of Chinese and Eurasian International Relations.* London: Routledge, p. 414.
[80] Koepp, Robert (2020). "Locating the Digital Silk Road in the Belt and Road Initiative," in Gordon, David, Nouwens Meia (2020). "The Digital Silk Road: China's Technological Rise and the Geopolitics of Cyberspace," *Adelphi Series*, Vol. 60(487–489), p. 38.
[81] Koepp, 2020, p. 44–45.

pillar of China's foreign policy and a means to promote the country's technological advancements and to expand Chinese influence over global digital networks.[82]

Table 1. The evolution of the DSR concept

Conceptual Term	Time	Occasion	Focus
Information Silk Road	March 2015	Vision and Actions on Jointly Building Silk Road Economic Belt and 21st Century Maritime Silk Road	Communication-network construction, especially optical cables
Online/Cyber and Digital Silk Road	July 2015	1st China–EU Digital Cooperation Roundtable in Brussels	Digitalisation, cyber development and cyberspace security
		15th Forum on Internet Media of China	
	Dec 2015	2nd World Internet Conference	
Online/Cyber and Digital Silk Road	March 2016	The 13th Five-year Plan	High-speed fibre-optic networks
Online/Cyber and Digital Silk Road	May 2017	The 1st BRI Forum	Innovation-driven development and frontier technologies
Digital Silk Road	April 2018	National Conference on Cyber Security and Informatisation	Network infrastructure construction, digital economy, network security, and other aspects
Digital Silk Road	April 2019	The 2nd BRI Forum	The fourth industrial revolution and the opportunities for digital, networked, and intelligent development

Source: Cheng, Jing, and Zeng, Jinghan (2023). "Digital Silk Road as a slogan instead of a grand strategy," *Journal of Contemporary China,* Vol. 33(149), p. 832.

[82] Gordon, David, Nouwens Meia (2020). "Introduction," in Gordon, David, Nouwens Meia (2020). "The Digital Silk Road: China's Technological Rise and the Geopolitics of Cyberspace," *Adelphi Series*, Vol. 60 (487–489), p. 13, 14.

Inherently, there is a connection between BRI and DSR, as any non-digital infrastructure project, spanning from high-speed railways to oil pipelines, relies on ICT to achieve system integration.[83] What the DSR adds to China's global ambitions is that it promotes the country's leading role in producing physical and virtual infrastructure in the digital sphere.

On the legal front, China does not regulate data governance in the same way as the EU and the US. The DSR lacks a legal framework for data security, and instead it operates under a complex web of non-binding soft-law instruments, such as Memoranda of Understanding (MoU).[84] The recipient country's data protection legislation is presumably the most important factor in determining how data is managed and what data may leave the country. Once data have left the recipient country, three key Chinese laws enable data to be centrally stored in China, namely, the Personal Information Protection Law, the Cybersecurity Law, and the Data Security Law. These laws grant the state extensive powers to centralise and use data collected by companies, originating from domestic as well as international customer bases.[85] Therefore, in practice, the DSR operates within a legal framework that provides the Chinese state with broad authority to override corporate data security provisions.

The DSR's geographical scope extends well beyond that of the BRI, as there are more countries considered recipients of the DSR compared with the BRI member states.[86] That a country becomes a recipient of DSR projects and technologies that fall under the broader definition of DSR does not necessarily mean that the country has signed an MoU with China.[87]

The DSR is carried out by a mixture of state-owned enterprises, such as ZTE, and private-sector tech companies, such as Alibaba. The former are primarily in charge of infrastructure projects, for example, network infrastructure construction, while the latter are mainly in charge of services and platforms.[88] The set of infrastructure and technologies that form the core of the DSR includes; telecommunications, artificial intelligence, economic platforms, financial services, data centres, and security systems (see also Section 1.2).

---

[83] Koepp, 2020, p. 47.

[84] Lagiewska, Magdalena (2024). "Legal aspects of the digital silk road: Trends and challenges," in Sahakyan, Mher (2024). *Routledge Handbook of Chinese and Eurasian International Relations*. London: Routledge, p. 414. See also Erie, Streinz, 2021.

[85] See Creemers, Rogier et al. (2022). *Translation: 14th five-year plan for national informalization.* DigiChina, Cyber Policy Center, Freeman Spogli Institute.

[86] Nouwens, Meia (2020). "Identifying the Silk Road," in Gordon, David, Nouwens Meia (2020). "The Digital Silk Road: China's Technological Rise and the Geopolitics of Cyberspace," *Adelphi Series*, Vol. 60(487–489), p. 53.

[87] In reality, the same can be true for BRI recipients, as seen in the example of Norway, which, although not officially a member of the BRI, has engaged in various forms of cooperation with China, including maritime partnerships and participation in the Asian Infrastructure Investment Bank.

[88] Nouwens, 2020, p. 54.

Two aspects of the DSR are important to note, however. First, the DSR did not result from a top-down process.[89] Chinese companies have long been active players in global digitalisation. The private-sector tech companies' activities happened to promote the geopolitical goals of the state, which in its turn capitalised on their success and folded the DSR into the BRI. The principal drivers of the DSR activities on the ground are the Chinese private-sector tech companies seeking commercial survival and rewards, while competing with one another for state support.[90] Second, the DSR concept itself lacks coherent and consistent specifics. It is instead a broad label used to encapsulate a vague idea of the Chinese government regarding anything digital.[91] Thus, the DSR should not be seen as an initiative or geopolitical objective that is centrally managed by Chinese ministries, nor as an all-encompassing concept that includes every business operation related to the digital economy under its umbrella. It should rather be seen as an overarching branding strategy that allows Beijing to showcase its global vision across various key technology sectors.[92]

2.2.1 Türkiye's incorporation into the DSR

China and Türkiye have engaged in multiple initiatives and partnerships under the BRI, which collectively have provided the framework for Türkiye's incorporation into the DSR.

Initially, the MoU signed in 2015 with the aim of aligning the BRI with Türkiye's Middle Corridor Initiative, laid the groundwork for future cooperation, including in the digital sector.[93] Later, at the 4th World Internet Conference (also known as the Wuzhen Summit) organised by China in 2017, China and seven other countries co-launched a digital economy cooperation initiative, with the aim of leveraging digital opportunities and boosting connectivity along the ancient Silk Road.[94] Türkiye was one of those countries and agreed to contribute to building an interconnected DSR.[95]

Recognising the need to close the digital divide, drive innovation, and spur economic development, the Turkish government began to embrace digital transformation. As part of the increased policy support for digital transformation, Türkiye signed an official DSR MoU with China.[96]

---

[89] See, for example, Cheng, Jing, Zeng, Jinghan (2023). "Digital Silk Road as a slogan instead of a grand strategy," *Journal of Contemporary China*, Vol. 33(149), p. 823–838.
[90] Gordon, Meia, 2020, p. 16–18.
[91] Cheng, Zeng, 2023, p. 826.
[92] Triolo, 2020, p. 66.
[93] Presidency of the Republic of Türkiye, Ministry of Foreign Affairs. Türkiye–People's Republic of China Economic and Trade Relations.
[94] Yiming, Guo (2017). "Digital economy cooperation to empower Belt, Road," *China.org*, 4 December.
[95] Eurasia Group (2020). *The Digital Silk Road: Expanding China's digital footprint.* Fudan University, p. 4.
[96] Aluf, Dale (2023). "China's digital footprint grows in the Middle East and North Africa," *Mapping Global China*, 8 June; Eurasia Group, 2020, p. 2.

In 2023, the Silk Road Fund and the Investment Office of Türkiye co-hosted a roundtable on China–Türkiye investment cooperation. The event highlighted the complementary nature of the countries' economies and the great potential for cooperation in, among other areas, the digital economy.[97] In the same year DEİK and the Turkish Industry and Business Association (TÜSİAD) organised the Türkiye-China business conference. At the conference, the countries agreed to deepen further existing cooperation in digital transformation, including areas such as e-commerce and telecommunications, and to initiate new partnerships in areas such as cloud technology.[98]

In 2024, high-level talks of the Türkiye–China Intergovernmental Cooperation Committee, the highest-level consultation mechanism between the countries, were held in Beijing, co-chaired by the Turkish Minister of Treasury and Finance and the Chinese Vice Premier. The meeting highlighted Türkiye's commitment to help China harmonise its Belt and Road initiatives and the country's commitment to Beijing's "One China" policy. The meeting also stressed Türkiye's sustained desire to strengthen cooperation with China on the digital front, infrastructure, and 5G-connectivity, and encouraged increased Chinese investments.[99]

In an attempt to bring investments under one roof, the Chinese state-owned company Lingang Shanghai Data Port and the China Trade Association based in Türkiye signed a cooperation agreement in 2024.[100] According to the agreement, a trade and technology centre will be established in Türkiye in the near future, with the goal of facilitating Chinese investment, enabling tech partnerships, supporting startups, and expanding AI and data collaboration.

Considering that the DSR lacks coherent specifics, it is hard to make a decisive assessment of the level to which Türkiye is incorporated into it. However, the aforementioned examples strongly indicate that Ankara is actively engaging with Beijing's ambitions to expand its influence over global digital networks.

[97] Silk Road Fund (2023). "Silk Road Fund and the Investment Office of the Presidency of Turkey Co-hosted the Roundtable on China–Turkey Investment Cooperation," 27 July.
[98] *Global Times* (2023). "Turkey–China business conference announced to strengthen cooperation in digital transformation," 13 July.
[99] *Anadolu Agency* (2024). "Türkiye–China meeting to foster regional, global peace and prosperity," 8 November.
[100] Yımlaz, Emirhan (2024). "Cooperation with Chinese state-owned company beginning of tech, trade base in Türkiye," *Anadolu Agency*, 10 August.

3 China's foothold in Türkiye's digital ecosystem

This chapter presents the empirical findings of the study. It first illustrates the sectoral distribution of the Chinese companies identified as engaging within Türkiye's digital ecosystem. Then it outlines some key Chinese investments and cooperation agreements, accompanied by an analysis of how these engagements indicate China's foothold in Türkiye's digital ecosystem. The chapter concludes with a discussion.

3.1 Areas of Chinese business engagement

As extensively described in Section 1.4, Material and Method, this study found 151 Chinese companies active within Türkiye's digital ecosystem. The areas in which these companies operate are presented in Table 2 below.

Table 2. Sectoral distribution of Chinese companies operating in Türkiye's digital ecosystem

Area	Number
Hardware	32
Manufacturing	47
Services—Telecommunications and Information Technology (IT)	30
Services—Financial	3
Wholesale and Retail	39
Total	151

Source: Author's own dataset.

The companies listed under Hardware include those active within telecom infrastructure, exemplified in the infrastructure section below. The second area lists manufacturing companies, which create and produce devices that range from security systems to communication equipment and electrical machinery relevant to the digital sector, to products relating to infrastructure, such as cables. Such manufacturing companies belong to both the section on infrastructure, and to all the subunits set out in the digital sector. The third area gathers those companies that provide services in the form of, for example, cellular communication (mobile services), internet and broadband services, cloud communication, cybersecurity services, and software development. These services are illustrated under all the different subunits of the digital sector. The companies listed under the fourth area are discussed under the Economic platforms and Financial Technologies subunit of the digital sector. Companies listed under the fifth area, Wholesale and Retail, deal with electronic devices or components, distributing or retailing them. Some

of the companies under this category install electronic systems in devices or are involved in assembling or manufacturing parts of devices. Those are, however, categorised under the Wholesale and Retail, instead of the Manufacturing area of operations, because they do not manufacture the whole device or product in question. The companies listed under Wholesale and Retail are illustrated under all subunits of the digital sector.

As already noted, many of the companies operate in more areas than the one under which they are listed. The listing was made, however, according to the companies' primary reported area of operations.

The section below provides some key examples of Chinese business engagement in the Turkish digital ecosystem's various subunits, to exemplify the firmness of the companies' presence, along with their ambition or capacity to shape the area in which the companies are operating.

3.2 Extent of Chinese business engagement

This section presents and analyses a handful of key Chinese business engagements within Türkiye's digital ecosystem, distributed across the subunits that emerged during the material processing.

3.2.1 Infrastructure

Chinese firms are important players in the infrastructure of telecommunications. Telecom is the transmission of information over a distance, usually via cables or radio waves. 5G is the fifth generation of mobile networks and therefore a part of telecom. Since fibre-optic cables form the backbone of telecom, the fibre-optic network itself could be considered a distinct pillar of infrastructure. However, based on publicly available information, no Chinese company appears to own any part of Türkiye's fibre-optic network directly.[101] Instead, Chinese firms act as suppliers and partners to Turkish telecom companies that maintain and develop the fibre-optic infrastructure and thereby enhance telecom performance. Consequently, this type of engagement is addressed in the next section.

Telecom

Türkiye's economic growth is highly reliant on the structure and development of the country's telecom sector. In line with global trends, Türkiye's population of

[101] TürkTelekom owns and maintains 78% of Türkiye's national fibre network. A few other companies, such as Turkcell, Turkstat, and Vodafone own the remaining portions; see, for example, Hayatsever, Huseyin, Tuncay, Ebru (2024). "Turkey mulls unifying telecom fibre infrastructure in one entity, official says," *Reuters*, 11 November.

almost 88 million favours mobile phones, which are progressively replacing land-line telephony. The three leading mobile operators in the country are Turkcell, Vodafone Türkiye, and TürkTelekom. Since 2019, Turkcell has been the dominant operator, holding approximately 40% of market share each quarter.[102]

China's telecom leader Huawei entered the Turkish ICT market in 2002, and has since provided multiple services. In telecom, Huawei has engaged with all three leading Turkish operators to varying extents. Since 2017, Huawei has signed a series of cooperation agreements with Turkcell for the development of next-generation wireless network technologies, culminating in MoUs in 2024 to develop 5G-Advanced (5G-A) networks and next-generation AI-supported systems.[103] Moreover, in 2020, Turkcell was the first foreign user of Huawei's mobile application infrastructure.[104] Currently, Huawei employs a team of over 750 engineers in its Research and Development (R&D) centre in Türkiye, which has become a key component of Türkiye's telecom infrastructure.[105]

China's ZTE Corporation conducts multiple data-speed trials with Türk Telekom, contributing to the development of next-generation data-transmission technologies and supporting the digital transformation of Turkish industries.[106] The largest investment ZTE has made in Türkiye, however, concerns the 2016 acquisition of a 48% stake in Netaş Telekomünikasyon A. Ş., making ZTE the company's single largest stakeholder. Netaş is Türkiye's leading systems integrator and ICT services provider.[107] Netaş has, among others, deployed communication infrastructure in Istanbul's new airport, provided ICT infrastructure to over 8000 schools and five hospitals, extended its capabilities in the enterprise market, offering solutions for large organisations and government agencies, supporting their e-government initiatives, and provided digital solutions to banks. It is hard to assess, through open sources, how much of the technology that Netaş has deployed is ZTE's technology. However, considering the large stake that ZTE owns in Netaş and the extensive outreach that Netaş, in turn, has in Türkiye's critical infrastructure, it is fair to infer that the Chinese company has considerable insight into that infrastructure.[108] In any case, this large investment by ZTE suggests both the company's firmly established presence and its capacity to shape the sector.

Moreover, Netaş is home to Türkiye's first private telecom R&D centre, and ZTE positions Türkiye as a localisation hub for its fibre broadband and telecom

[102] Dierks, Zeynep (2025).
[103] Guliyev, Vusal (2024). "Turkish–Chinese rapprochement: Growing Chinese investment in Turkiye," *Caspian–Alpine Society*, 3 December.
[104] Sezer, Can (2020). "Turkey's Turkcell signs deal to use Huawei's mobile services," *Reuters*, 12 February.
[105] Huawei (2022). "Huge collaboration in 5G from Turk Telekom and Huawei," 12 March.
[106] See, for example, ZTE (2024). "Türk Telekom and ZTE conduct Europe-first 3-in-1 50G PON Combo trial in Türkiye." 19 March; *Mobile World Live* (2025). "Türk Telekom and ZTE complete the world's first 1.6T with 12THz bandwidth DWDM trial on a live network," 4 April.
[107] *Anadolu Ajanci* (2016). "Chinese ZTE buys stake in Turkey's Netas for $101M," 6 December.
[108] Presidency of the Republic of Türkiye. Investment and Finance Office. Success Stories: Netaş.

solutions.[109] Netaş localises ZTE's solutions, which means that Chinese-designed equipment is either manufactured or assembled in Türkiye. This means that Turkish carriers can deploy ZTE-enabled infrastructure with Turkish-built hardware, which in turn embeds Chinese technology within Türkiye's own telecom fabric. ZTE's influence via Netaş extends into managed services, technical support, field services, and training, as well as smart city and ICT integration.[110] Thus, beyond direct hardware and shaping network components, ZTE is engaged in Türkiye's operational practices and service delivery. The ZTE–Netaş partnership is framed by officials as one that will serve the entire region, suggesting long-term engagement ambitions and that the Chinese company can use Türkiye as a stepping-stone for broader regional telecom deployments in the future.[111]

Overall, the ZTE–Netaş partnership involves Chinese ownership, joint R&D, localised manufacturing, infrastructure deployment, service integration, and regional expansion. Apart from exporting telecom gear, this partnership embeds Chinese telecom expertise, control, and influence into the Turkish telecom ecosystem.

Other than Huawei and ZTE, multiple other Chinese smartphone manufacturers such as Xiaomi, OPPO, Vivo, and Tecno Mobile have begun local production in Türkiye, with factory investments ranging between USD 20–35 million.[112] While smaller in scale, these operations assist in localising supply chains and support Türkiye's domestic tech ecosystem, while strengthening China's foothold in the critical sector of telecommunications.

Huawei's extensive investments in R&D facilities in Türkiye suggest the company's desire to establish a local presence and drive technological advancement within Türkiye. Huawei's R&D and Software Solutions Centre in Istanbul, the company's second-largest outside China, is vital for supporting Türkiye's broader 5G ambitions. The centre focuses on advancing telecom technology, developing new hardware and software solutions, and improving the efficiency of 5G networks in Türkiye.[113] The company has invested more than USD 150 million in the centre in total funding, with roughly USD 20 million spent annually.[114] This

[109] Ibid.
[110] Ibid.
[111] Şimşek, Bariş (2017). "Turkish, Chinese telecom partnership looks to provide technical infrastructure for Belt and Road project". *Daily Sabah*, 5 December.
[112] See, for example, *Bazaar Times* (2022). "Technology brand Vivo continues to invest in Türkiye," 15 December; *Daily Sabah* (2021). "China's Techno Mobile starts production at Turkey factory," 24 May; *Daily Sabah* (2021). "Chinese Xiaomi to begin smartphone production in Turkey," 4 February; OPPO (2021). "Türkiye'deki Fabrikasında Üretime Başlayan OPPO, Global Üretim Kapasitesini Artırdı" [OPPO, which started production in its factory in Turkey, has increased its global production capacity], 12 July.
[113] Huawei (2025). Turkey Research and Development Center.
[114] Huawei (2025). Turkey Research and Development Center; Presidency of the Republic of Turkiye. Investment and Finance Office. Huawei.

kind of engagement suggests ambitions for long-term presence and for being an essential actor in shaping Türkiye's 5G networks.

When it comes to infrastructure deployment, Huawei has supplied 5G equipment, such as base stations, antennas, and cloud software, to Turkish telecom companies such as Vodafone Türkiye, Türk Telekom, and Turkcell. An example of Huawei's cooperation with Vodafone Türkiye was the launching of the TechCity 2.0 project in 2017, where the companies jointly tested advanced technologies, such as 4x4 Multiple-input Multiple-output (MIMO) antenna technology in Istanbul, with the aim of enhancing connectivity in high-density areas. 4x4 MIMO is an important component of 5G technologies.[115] This deployment required physical Huawei equipment to be installed in key urban areas in order to display real 5G performance. Moreover, the project required high-capacity, reliable connectivity, which is generally supported by fibre-optic networks. Thus, Huawei provided hardware and technology that underpin the fibre-optic infrastructure used in the project.

An example of Huawei's collaboration with Türk Telekom was the agreement to develop and test industrial 5G applications in 2022.[116] This kind of deployment generally requires a real, working 5G network environment consisting of, among other things, base stations and core network components, as well as software infrastructure. Thus, to develop and test 5G applications, Türk Telekom deployed Huawei's equipment in parts of its network.

Lastly, an example of cooperation between Huawei and Turkcell is the agreement to build a 5G global-scale cloud-native core network in 2019.[117] The cloud-native component means that the network is built to run in the cloud, so that it is not tied to any specific location or physical servers, enabling flexibility, scalability, and easy updates. The cooperation requires that Huawei supply cloud-native core network software and hardware that manage data traffic and signalling, which are integrated into Turkcell's 5G systems.

Another example is the agreement to explore the latest iteration of 5G technology, green energy solutions, and AI-driven network automation in 2024.[118] This involves at least some degree of technical implementation, suggesting that Huawei's role will likely extend beyond that of a research partner to include functions typical of an infrastructure provider. On some occasions, systems that Huawei has jointly produced with Turkcell have been deployed in Türkiye's critical infrastructure, for example in Istanbul's new airport.[119] Thus, these examples of collaborations and Huawei's engagement with 5G infrastructure in Türkiye suggest the company's

[115] Huawei (2017). "Huawei and Vodafone Turkey Sign the TechCity 2.0 MoU," 9 June.
[116] Huawei (2022). "Huge collaboration in 5G from Türk Telekom and Huawei," 12 March.
[117] Huawei (2019). "Turkcell Joins Hands with Huawei to Build a 5G-oriented All-Cloud Core Network," 15 February.
[118] Huawei (2024). "Turkcell and Huawei signed three MOUs on 5.5G, green energies, and AI based networks at MWC 2024," 29 February.
[119] *RCR Wireless News* (2018). "Huawei launches in-building 5G at Istanbul's new airport," 27 November.

foothold in Türkiye's 5G infrastructure, as it provides both the technology and expertise required for building out the networks.

Though to a lesser degree than Huawei, ZTE has also provided 5G infrastructure to telecom operators. An example of cooperation between ZTE and Turkish operators is ZTE's involvement in core and metro optical network updates. The core network connects major cities over long distances, while the metro network covers local areas within cities, linking neighbourhoods and businesses to the core. ZTE supplied advanced optical transport technology and assisted Türk Telekom in expanding its metro optical transport network in Istanbul to support very high speeds, enabling it to handle increasing 5G traffic demands.[120] ZTE also assisted Turkcell with building an advanced metro optical transport network in Bursa.[121] By upgrading Turkish operators' core and metro optical networks with advanced technologies, ZTE is supplying critical backbone fibre-optic infrastructure that carries and manages 5G data traffic. This confirms that ZTE's equipment and technology are deployed and used within Türkiye's 5G network, highlighting China's foothold in Türkiye's fibre-optic development. The provision of upgrade services also suggests future lock-in effects; by exporting Chinese technologies and standards, ZTE creates a Turkish dependency on them, prolonging the company's presence in Türkiye's digital ecosystem.[122]

Another example is Türk Telekom and ZTE deploying Europe's first millimetre-wave 5G-A integrated sensing and communication (ISAC) solution in Türkiye's Kumport port (65% of which is owned by the Chinese state-owned company COSCO) for real-time vessel tracking and safety monitoring.[123] This system uses fast 5G wireless technology (millimetre-wave) to not only communicate data but also to sense the environment around it. This engagement suggests that ZTE's millimetre-wave active-antenna systems and advanced radio hardware were integrated into Türk Telekom's live network in a critical sector for Türkiye's maritime security.

A last key engagement is ZTE and Turkcell's agreement to cooperate in driving 5G-A and 6G technologies, including 5G fixed wireless access, private enterprise networks, green network solutions, and ISAC technologies.[124] As in the previous examples, this initiative requires that Turkcell deploy ZTE's testbed infrastructure. Thus, apart from suggesting ZTE's firm presence in Türkiye's 5G infrastructure,

[120] *Mobile World Live* (2022). "ZTE assists Turk Telekom in core sites expansion of 100G&B100G metro optical network," 5 July.
[121] Sharma, Ray (2022). "ZTE, Turkcell Deploy 'World's First' Commercial 12THz WDM System," *The Fast Mode*, 6 June.
[122] For more on lock-in effects see, for instance, Rühlig, Tim (2020). *Technical standardisation, China and the future international order: A European perspective.* Heinrich Böll Stiftung.
[123] ZTE (2025). "Türk Telekom and ZTE launch Europe's first millimeter-wave supported 5G-A ISAC maritime management solution," 10 March.
[124] ZTE (2025). "ZTE and Turkcell sign MoU to drive 5G-A innovation," 10 March.

the examples above also suggest the ambition to maintain and deepen that presence in the future.

The survey of the infrastructure segment of Türkiye's digital ecosystem suggests a strong Chinese foothold, not only through equipment provision and direct infrastructure deployment but also via service integration, manufacturing, and agreements for the future development of advanced and next-generation technologies that support this infrastructure. These elements signal potential future lock-ins, as the provision of Chinese technologies and standards to Turkish actors makes them dependent on companies that use those technologies and adhere to those standards—namely, Chinese companies.

3.2.2 Digital sector

The digital sector encompasses economic platforms and financial technologies, cloud computing, and smart-city technologies. As was the case with infrastructure, the various subunits here are not isolated, rather, they are often interconnected.

Economic platforms and financial technologies

Unlike infrastructure, e-commerce, as a form of soft-power economic penetration, allows China to project influence digitally.[125] In 2024, e-commerce platforms accounted for about 20% of total retail sales in Türkiye, with the e-commerce volume increasing by 275% since 2019.[126]

Alibaba's acquisition of the majority share of Trendyol, Türkiye's e-commerce titan, is the largest Chinese investment in Türkiye's e-commerce sector. In 2018, Alibaba acquired this share with the investment of USD 730 million.[127] In 2021, Alibaba invested another USD 350 million in Trendyol, elevating its ownership to 86.5%.[128] This gives China end-to-end control of vital digital infrastructure in Türkiye, as Alibaba gains access to consumer data, merchant data (e.g., supply chain and inventory), logistics infrastructure (e.g., warehousing and returns), and payment channels. In general, Chinese firms like Alibaba do not enter markets solely as online marketplaces. Instead, they act as vectors of economic penetration, as they bring with them AI-driven analytics, recommendation engines, and logistics and supply-chain platforms, in order to embed Chinese technological

[125] Choudary, Sangeet, Paul (2020). "China's country-as-platform strategy for global influence," *Brookings*, 19 November.
[126] *Daily Sabah* (2025). "Türkiye's e-commerce volume reached $90B in 2024: Trade minister," 6 May.
[127] AEI (2024). China Global Investment Tracker. "Chinese investments and contracts in Turkey (2005–2024)"; Primack, Dan (2018). "Scoop: Alibaba paid $750 million for Turkish startup Trendyol," *Axios*, 14 August.
[128] AEI (2024). China Global Investment Tracker. "Chinese investments and contracts in Turkey (2005–2024)"; *Daily Sabah* (2021). "Alibaba invests $350M in capital increase to Turkey's Trendyol," 21 April.

standards within the host country's digital infrastructure.[129] In this direction, in 2023, Alibaba committed to a USD 2 billion expansion package for Trendyol, to scale operations and build a data centre and a logistics centre in Ankara, as well as an export centre in Istanbul's airport.[130] This reveals Alibaba's forward-looking commitment to deploy its set of technologies and software solutions to enhance further Türkiye's digital infrastructure, and, as Alibaba's President stated, "Make Türkiye part of the company's supply chain in Europe, Middle East, and Far East."[131] The company's strong presence, with the ambition to remain and the capacity to shape the entire e-commerce sector, thus becomes evident.

The e-commerce and fintech sectors, though operationally separate, are mutually reinforcing and allow Chinese companies to embed themselves digitally in foreign markets.[132]

Alibaba has rolled out its payment system, Alipay, in Türkiye, primarily to serve Chinese tourists, through partnerships with Turkish fintech firms and banks. An example of such a deployment is Turkish fintech company Ininal signing a cooperation agreement and becoming the first Turkish partner of Alipay in 2019.[133] The agreement included the establishment of the necessary network and infrastructure, which would facilitate the expansion of Alipay into sectors beyond tourism.[134] Another example of such a deployment is Türkiye İş Bankası integrating Alipay into its online and point-of-sale (POS) systems, facilitating e-commerce and in-store payments for Chinese consumers.[135] By 2024, Türkiye İş Bankası had upgraded to Alipay+, enabling e-wallets at over 500,000 POS terminals nationwide, including at Istanbul airport.[136] These two examples, apart from bringing Chinese payment culture into daily retail and boosting economic flows between China and Türkiye, help integrate Türkiye's payment infrastructure into Alibaba's global network. There are more Chinese firms than Alibaba that have embarked on similar journeys. For instance, China's Tencent, the world's largest gaming company, launched its payment platform WeChat Pay at Istanbul airport in 2020.[137]

---

[129] See, for instance, Vecchi, Alessandra, Brennan, Louis (2022)."Two tales of internationalization—Chinese internet firms' expansion into the European market," *Journal of Business Research,* Vol. 152, p.106–127.
[130] Attarwala, Fatima (2023). "Alibaba expands international business with 2 billion investment in Turkey's Trendyol", *Investopedia*, 18 September.
[131] *Data Center Knowledge* (2023). "Bloomberg News: Alibaba Plans logistics hub at Istanbul airport, data centre near Ankara," 9 January.
[132] Nagel, Avi (2021). "E-commerce integration in China," *The FinTech Times,* 18 March.
[133] *Bloomberg HT* (2019). "Ödeme platformu ininal, Alipay'in Türkiye'deki ilk iş ortağı oldu" [The payment platform ininal became Alipay's first partner in Türkiye], 21 May.
[134] Ibid.
[135] *Daily Sabah* (2019). "Turkey's İş Bank, China's AliPay expand cooperation on payment systems," 25 December.
[136] *Finextra* (2024). "İşbank expands partnership with Alipay+," 20 December.
[137] Celik Gözde (2020). "WeChat Pay launches service in Turkey targeting Chinese tourists," *KrAsia,* 29 July.

China has no equity stake in Turkish fintech firms at present. Moreover, the aforementioned initiatives in the fintech sector are mainly targeting Chinese tourists and have not yet expanded widely among Turkish users. However, Alipay's integration through Ininal and İş Bankası mark a clear case of digital penetration by the Chinese fintech ecosystem in the Turkish market, leveraging payments infrastructure to project fintech influence in Türkiye.

In line with previous research on Chinese influence, this study finds that even in the case of Türkiye, China's engagement with economic platforms and financial technology involves exporting platforms (Alibaba), rolling out payment systems (Alipay, WeChat Pay), and establishing logistics networks, e-commerce hubs, and data infrastructure.[138] Although business presence has not yet developed into a foothold in the fintech sector (see Section 1.2 for the scale), a Chinese business foothold is certainly established in the e-commerce sector.

Cloud computing

Unlike physical infrastructure, penetration of cloud-based services allows non-physical but foundational control over data flows, hosting, and computation.

In 2018, Alibaba Cloud, the cloud arm of Alibaba Group, partnered with Turkish services company E-Glober to introduce cloud services in Türkiye.[139] By collaborating with E-Glober, Alibaba gained a localised gateway into Türkiye without needing an independent corporate presence. This cooperation agreement's significance lies in the fact that Alibaba Cloud became a key player in Türkiye's public cloud space. By entering early and partnering locally, Alibaba Cloud has become influential among Turkish enterprises looking for affordable cloud options.[140] The scope of this partnership was to help Turkish enterprises strengthen their cloud applications and offer them access to *elastic compute* (the ability to adjust computing resources dynamically, such as storage, based on demand), databases, networking, security, analytics, and big-data tools, a scope well beyond raw storage.[141] These cloud services are now delivered under a Chinese technology framework, directly integrating Alibaba's set of technologies, tools, and programming languages into Turkish digital operations. The platform-level services

[138] For previous research on this topic, see, for instance, Raymond, Peter (2023). "Re-platformed planet? Implications of the rise and spread of Chinese platform technologies," *CSIS*, 29 March; Choudary, Sangeet, Paul (2020). "China's country-as-platform strategy for global influence," *Brookings*, 19 November; Zhang, Longmei, Chen, Sally (2019). "China's digital economy: Opportunities and risks," *IMF e-library*, 17 January; Vanberghen, Christina (2025). "How Beijing's digital strategy is reshaping global rules—and what Europe should do about it," *Modern Diplomacy*, 25 May.

[139] E-Glober is acting as a local bridge for both e-commerce exports (via Alibaba.com) and cloud computing (via Alibaba Cloud). For more about E-Glober, see, for instance, *The Brand Age* (2015). "Alibaba.com'un Türkiye'deki Yeni İş Ortağı Mehmet Ali Yalçındağ'ın E-Glober'ı Oldu" [Mehmet Ali Yalçındağ's E-Glober becomes Alibaba.com's new business partner in Turkey], 30 November.

[140] GMI Research (2021). "Turkey cloud computing market share, size and industry growth report, 2020–2027"

[141] Alibaba Cloud (2018). "Alibaba Clouds expands into Turkey," 9 April.

that Alibaba Cloud delivers become embedded in a Turkish company's core infrastructure. Once embedded, switching costs become high, increasing the chances that Turkish companies become dependent on Chinese cloud standards and service models. This creates long-term technological lock-in.[142]

China's long-term outlook with this type of engagement becomes evident when considering cloud penetration in tandem with the e-commerce sector; Alibaba owns the majority share of Trendyol. Alibaba Cloud supports Trendyol, Trendyol's growth necessitates localised cloud expansion, and expansion feeds deeper cloud penetration across Türkiye. A self-reinforcing loop manifests, revealing the way in which Chinese standards embed themselves into Turkish digital ecosystems. The parallel growth of e-commerce and cloud sectors is supported further by the fact that Alibaba plans another USD 1 billion investment in Türkiye for a logistics hub and a data centre.[143] This signals deep infrastructural integration that aims to anchor Alibaba Cloud's regional presence.

Following Alibaba's example, Huawei has notably expanded its presence in Türkiye's cloud sector since 2023. In July that year, Huawei officially entered the Turkish public cloud market by launching its first localised cloud, physically located in Türkiye, hosted in local data centres, with data stored and processed locally.[144] Within a year, Huawei Cloud saw a 12-fold growth, serving over 360 Turkish enterprises in a wide range of sectors, including banking, e-commerce, and media; critical sectors that hold sensitive data.[145]

Moreover, partnering with universities and startups, Huawei launched its "Cloud acceleration programme for digital transformation" in 2024, committing USD 6 million in credits and resources to support Turkish startups' cloud migration.[146] An important aspect of this initiative is its focus on AI-native infrastructure, which is set to integrate AI across data centres, development, and operations (Cloud for AI and AI for Cloud).[147] By promoting AI-native infrastructure, Huawei is establishing technical standards for next-generation enterprises in Türkiye. Generally, government agencies, telecom operators, and major corporations use these kinds of services. This means that key public and private institutions are building digital infrastructure on Huawei's architecture, which shows how the Chinese company embeds itself in Türkiye's digital ecosystem through technological standards.

---

[142] For more on cloud vendor lock-in and service lock-in, which makes migration to another provider complicated and expensive, see, for instance, Opara-Martins, Justice (2018). "Taxonomy of cloud lock-in challenges" in Khatib, Mutamed, Salman, Nael (2018). *Mobile computing—Technology and applications*. InTech; Alhosban, Amal, Pesingu, Saichand, Kalyanam, Krishnaveni (2024). "CVL: A cloud vendor lock-in prediction framework," *Mathematics*, Vol. 12(3), 387, p. 1–18.

[143] *Al Arabiya English* (2023). "Alibaba plans $1bln logistics hub at Istanbul airport, data centre near Ankara," 8 January.

[144] *Huaxia* (2023). "China's tech giant Huawei launches localized cloud in Türkiye," 13 July.

[145] Huawei Cloud (2024). "Huawei Cloud Unveils AI-Native Cloud, Becoming the Preferred Cloud of Turkish Leading Enterprises," 10 October.

[146] Ibid; Presidency of the Republic of Türkiye. Türkiye's FDI Landscape at a glance 2024, p 296.

[147] Ibid.

Considering the outlook of China's engagement ambitions, this initiative signals long-term dependencies, as aligning digital operations with Huawei's standards can lead to technological lock-in in the future.

In 2024, Huawei Cloud forged a partnership with Logosoft as its exclusive distributor in Türkiye and Europe, expanding Huawei's reach through a network of over 500 local partners.[148] By offering localised technical training, support, and sales, Huawei become part of the digital service-delivery architecture. This is another marker of Huawei entrenching itself in Türkiye's ICT infrastructure. Some months later, Hepsiburada, one of Türkiye's e-commerce giants, signed a collaboration agreement with Huawei Cloud and migrated its operations to the platform, with the aim of optimising latency, security, and costs via local data centres.[149] This partnership indicates robust adoption by a leading Turkish player in e-commerce, cementing Huawei's relevance in this type of critical infrastructure. As large Turkish firms build their entire digital stack on Huawei Cloud, it reinforces Huawei's role as an indispensable infrastructure provider.

More Turkish firms are following this example and deepening China's presence in Türkiye's cloud sector through localised infrastructure integration and technology transfer. An example is China's ZTE deepening its partnership with Turkcell and Netaş in 2025, after signing an agreement with the aim of supporting Turkcell's growing network demands.[150] This cooperation entails investment in, among other things, integrating next-generation technologies into Turkcell's Telco Cloud infrastructure and enhancing server capabilities.[151] This enhanced cooperation has upgraded server infrastructure, introduced hardware that can process data locally, and has amplified local manufacturing capacity. ZTE is the single largest shareholder in Netaş (see Section 3.2.1 on Telecom). Netaş expanded production in Istanbul for Netaş Cloud servers using ZTE-based technology under Turkish branding.[152] These servers are integrated into Turkcell's Telco Cloud infrastructure, empowering cloud operations. In this way, Chinese hardware is being manufactured and deployed locally, becoming a part of Türkiye's cloud backbone. Thus, the latest cooperation development signifies a shift from initial cloud-hardware entry to deep structural embedding of Chinese cloud technology within Türkiye's telecom and cloud infrastructure.

[148] Huawei (2024). "Türkiye'de daha güçlü bir bulut bilişim ekosistemi için Huawei Cloud ve Logosoft'tan stratejik ortaklık" [Strategic partnership from Huawei Cloud and Logodoft for a stronger cloud computing ecosystem in Turkiye], 22 February.
[149] Huawei Cloud (2024). "Hepsiburada Aims to Enhance Efficiency by Optimizing Costs with Huawei Cloud," 18 October.
[150] ZTE (2025). "ZTE, Netaş, Turkcell strengthen collaboration with server innovations and localisation efforts," 21 March.
[151] Ibid.
[152] Netaş (2022). Netaş annual report 2022.

Altogether, examining the cloud computing subunit of Türkiye's digital ecosystem suggests that, even here, Chinese companies are strengthening their foothold through infrastructure and ecosystem partnerships.

Smart city technologies

Given the broad scope of smart-city infrastructure, several Chinese forms of engagement can be considered relevant to its development and support. However, when it comes to Chinese engagement with Türkiye's smart-city sector as a whole, two examples stand out. In 2018, Huawei signed a smart-city collaboration agreement with Turkcell, beginning in Samsun and extending to wider applications.[153] This partnership encompasses 5G, network technologies, and industry-specific solutions in areas such as transportation, water management, and agriculture.[154] The agreement paved the way for co-development of sector-specific digital services tailored to municipal needs, even in critical sectors such as water management. This embedded Huawei's telecom and network technologies into Türkiye's urban digital infrastructure. In 2025, the companies signed an MoU to develop jointly next-generation smart-city infrastructure using 5G-A technology, quantum encryption, and autonomous network innovations.[155] This moved Huawei from a partner in vertical smart-city services to architect and innovator of Türkiye's urban connectivity stack. Chinese influence is thus embedded across infrastructure design, network protocols, and security standards.

Another example is the agreement signed in 2019 between Huawei and the Turkish Industry Technopark (Informatics Valley) for establishing an R&D centre within the technopark in Kocaeli.[156] As per the agreement, cooperation focuses on smart mobility technologies, AI, Internet of Things (IoT), and big data, strategic areas that Ankara generally prioritises.[157] This partnership between Huawei and a state-backed technopark indicates how the Chinese company is not only present in Türkiye's digital ecosystem, gaining market access. Rather, it actively co-develops next-generation technologies with Turkish national research actors, fostering knowledge transfer and standards adoption, and entrenching itself in local innovation pipelines.

Huawei's operations in the Koaceli-based technopark could complement the company's operations in the Istanbul-based R&D centre (see Section 3.2.1). Smart cities require both infrastructure and urban applications. These two R&D nodes (core tech development in Istanbul and urban application piloting and co-

[153] *ANews* (2018). "Turkcell, Huawei sign deal on smart cities in Turkey," 24 October.
[154] Ibid.
[155] Huawei (2025). "Turkcell and Huawei Sign Memorandum of Understanding for Leading Network Joint Innovations at MWC 2025," 4 March.
[156] *Daily Sabah* (2019). "Turkey, Huawei sign cooperation protocol on R&D for smart cities," 29 March.
[157] See for instance Presidency of the Republic of Türkiye, Presidency of Strategy and Budget. Twelfth development plan (2024–2028); Presidency of the Republic of Türkiye, Digital Transformation Office. National Artificial Intelligence Strategy 2021–2025.

development in Kocaeli) could, therefore, be viewed as parts of a coherent Huawei smart-city pipeline, embedded within Türkiye's national tech agenda. The blend of core platform development with applied urban innovation reflects a layered form of integration, where China's digital presence supports and shapes national priorities, particularly in AI, smart mobility, and cloud technology, all of which are pillars of Türkiye's digital and smart city ambitions.

SIS are a subset of smart-city infrastructure. Similar to other governments in the region, after the Gezi protests in Türkiye and general regional turmoil in the early 2010s connected to the Arab Spring, Ankara started to invest heavily in sophisticated equipment falling into the category of SIS, with the aim of monitoring, analysing, and tackling online and offline dissent.[158]

An example of Chinese engagement with Türkiye's national surveillance and smart-city ecosystems regards the Chinese firm Dahua. By holding roadshows since 2018, Dahua has demonstrated its interest in positioning itself as a provider of integrated citywide security systems in Türkiye.[159] Dahua has commercial and operational presence in Türkiye via its subsidiary, Dahua Turkey, which acts as a local distributor and systems integrator. That presence enables the company to secure tenders and maintain long-term integration in Turkish systems.

In 2019, Dahua officially entered Türkiye's critical security space after signing a technology transfer deal with the Turkish company ASİSGUARD.[160] The Turkish company operates in the fields of defence and border security as well as urban surveillance with armed drones, electro-optics, military vehicle modernisation, and AI capabilities.[161] The scope of the technology transfer deal concerns the co-development of thermal surveillance systems and high-tech cameras for public security, manufactured locally in Türkiye.[162] It is hard to assess via open sources into which of ASİSGUARD's products Chinese technology has been embedded. However, ASİSGUARD's latest electro-optical surveillance system, called AGGÖZ, which has been developed since 2019 and will be deployed on Turkish

[158] Yilmaz, Ihsan, Mamouri, Ali, Morieson, Nicholas, Omer Huhammad (2025). *The Transnational Diffusion of Digital Authoritarianism: From Moscow and Beijing to Ankara*. European Centre for Populism Studies, 12 May. The Gezi Park protests began in May 2013 in Istanbul as a sit-in against the demolition of Gezi Park but quickly escalated into nationwide anti-government demonstrations. Protesters criticised perceived authoritarianism, police brutality, and restrictions on civil liberties. For more on these protests, see, for instance, Gençoğlu Onbaşi, Funda (2016). "Gezi Park protests in Turkey: from 'enough is enough' to counter-hegemony?" *Turkish Studies*, Vol. 17(2), p. 272–294.

[159] *The Middle Eastern Security Market* (2018). "Dahua attracts new business with international roadshows," 22 November.

[160] Kunt, Rasim, Anil (2019). "Asisguard İle Dahua Teknoloji'den kamu güvenliği adına önemli anlaşma" [Important Agreement for Public Security Between Asisguard and Dahua Technology], *DefenceTurk*, 1 May.

[161] ASISGUARD (2025). About us.

[162] Kunt, 2019.

military drone platforms, has core thermal components and integration modules, likely utilising Dahua technology.[163]

This deal's significance lies in the fact that it enables the two companies to jointly develop and manufacture high-tech surveillance systems. This makes Dahua's technology part of Türkiye's security systems, and incorporates Chinese hardware and software into critical Turkish security platforms. Importantly, the surveillance technology co-developed through this deal is utilised in public-space monitoring, government buildings, and potentially also on military platforms. Thus, Dahua's technology is used by state authorities in critical security and likely defence contexts.

Hikvision, whose largest shareholder is CETC; one of China's leading defence conglomerates, is another example of a Chinese firm that has supplied surveillance equipment to Türkiye across multiple sectors, showing a substantive physical and institutional presence in the country's security ecosystem. As early as 2010 Hikvision had installed over 2000 network-based digital video recorders in all branches and ATMs of Turkish Ziraat Bank, providing monitoring and video retrieval.[164] In 2013, local security-solution integrator Kent Güvenlik Sistemleri A.Ş. installed Hikvision cameras, digital video recorders, and software at 240 rural Turk Telekom cellular-tower sites, with the aim of securing infrastructure across Türkiye's mountainous regions.[165] Moreover, Hikvision installed a comprehensive surveillance system, consisting of 545 camera channels, access control panels, network video recorders, and a central management system, in Ankara Metro Mall.[166] The security team planned to expand the surveillance system to the nearby residential area.[167] In 2016, Hikvision also established its Turkish subsidiary.[168]

These deployments illustrate how Hikvision has become a trusted supplier for major security projects, integrating its systems into Türkiye's public and commercial surveillance infrastructure. Even when in law enforcement, tender documentation from 2016–2018 shows Hikvision models in police procurement.[169]

---

[163] Özkan, Sedef (2022). "Asisguard 2022'de sınır güvenliğine odaklanıyor" [Asisguard focuses on border security in 2022], *BT Haber*, 4 April; Yildirim, Goksel, Yildirim, Emir (2025). "Turkish defense industry's new 'national eye' gimbal Aggoz empowers UAVs," *Anadolu Agency*, 4 March.

[164] *AsMag* (2010). "Hikvision Upgrades Turkish Ziraat Bank Surveillance Systems," 28 January.

[165] *The Global Security Market* (2013). "Hikvision overcomes terrain to secure Turkish telecom," 29 October.

[166] Hikvision (2020). Ankara Metro Mall Surveillance Project.

[167] Hikvision (2020). "Hikvision: securing one of the busiest shopping malls in Turkey's capital," 1 September.

[168] Alalouff, Ron (2018). "The spectacular rise of the Chinese video surveillance industry," *IfsecGlobal*, 7 March.

[169] See, for instance, Kamu Ihale Kurulu Kararlarıç 2019/323197 İhale Kayıt Numaralı "Afyonkarahisar İl Emniyet Müdürlüğü ve Farklı Lokasyonlardaki Çevre Güvenlik Kamera Sistemi Yapım İşi" İhalesi—Tarih: 24.10.2019 - No: 2019/UY.II-1380, [Public Procurement Board Decisions. Tender Registration

There is no publicly available official contract-award document confirming the final purchase and deployment of the specific models. However, Hikvision cameras have reportedly been seen at political rallies in Türkiye, operated by police officers.[170]

Other than these companies' extensive outreach, there are more Chinese firms with a presence in Türkiye's security-information-systems landscape. For instance, Nuctech signed two agreements, in 2017 and 2023, with Türkiye's Istanbul Airport and Sabiha Gökçen Airport to provide inspection equipment and explosive-detection scanners.[171] Airport and customs inspection systems are vital to national border security. Although these deployments are not as extensive as Dahua's and Hikvision's, inspection scanners often feed into wider security-monitoring networks and surveillance infrastructure, adding a layer to Chinese companies' entrenchment in the Turkish security-information-systems landscape.

Thus, the survey of the segment concerning smart-city technologies within Türkiye's digital sector suggests a layered integration of Chinese actors into Türkiye's urban digital and surveillance infrastructures, both of which encompass critical sectors and involve sensitive data.

3.3 Conclusions about China's foothold in Türkiye's digital ecosystem

In order to assess the areas and extent of China's engagement in Türkiye's digital ecosystem, this study examined the engagement, in the form of investments and cooperation agreements, of key Chinese stakeholders in its infrastructure and digital sector. When it comes to infrastructure, the study finds that in telecommunications, the Chinese presence is extensive and well-rooted, clearly signifying a foothold.

Chinese firms actively participate in, and integrate technologically, Türkiye's fibre-optic network through partnerships and projects that support telecom operations. The present analysis demonstrates that Chinese firms engage with all three major Turkish telecom operators to varying degrees. Engagement in telecom ranges from Chinese firms developing Türkiye's next-generation AI-supported networks and data transmission technologies, to Chinese infrastructure deployment in hardware, and even to service integration, with the ambition of using

Number 2019/323197 "Afyonkarahisar Provincial Police Department and Perimeter Security Camera System Construction Work in Different Locations" –Date: 24.10.2019 – No: 2019/UY.II-1380].

[170] See, for instance, Gostoli, Ylenia (2025). "Turkey's AI-powered protest crackdown," *New Lines Magazine*, 5 June.

[171] *Xinhua Net* (2017). "Istanbul new airport to use Nuctech-made inspection equipment," 29 December; *Ray Haber* (2023). "Security Systems are being Renewed at Sabiha Gökçen Airport," 20 October.

Türkiye as a base for wider regional telecom deployments in the future. What has facilitated the entrenchment of Chinese presence in Türkiye's telecom sector is that, apart from low-to-medium-scale investment and agreements on manufacturing, and supplying telecom equipment and network infrastructure projects, a Chinese stakeholder has gone as far as becoming the single-largest shareholder of Türkiye's leading systems integrator and ICT services provider, Netaş. This has facilitated Chinese technology penetration into multiple digital sectors and critical infrastructure in Türkiye, including government agencies, hospitals, banks, and schools.

Considering 5G, Chinese engagement largely focuses on driving technological advancement, supplying equipment that integrates Chinese standards with Türkiye's fibre-optic network and developing advanced, next-generation technologies. Chinese firms act as infrastructure providers, supplying 5G equipment to the main Turkish telecom companies and deploying that equipment within Türkiye's critical infrastructure and key urban areas. Cooperation agreements and large investments, especially in R&D, entrench Chinese presence in Türkiye's 5G sector and pave the way for long-term dependencies. Türkiye's telecom sector as a whole shows clear signs of Chinese ownership and/or operational control of the infrastructure, and thus reflects an established Chinese foothold in the sector.

In the digital sector, the scope of Chinese engagement is as strong as it is within infrastructure, highlighting Chinese penetration in Türkiye's digital ecosystem. First, when it comes to e-commerce, major Chinese investments have granted the country comprehensive oversight of Türkiye's critical digital infrastructure. Through Alibaba, this includes access to consumer and merchant data, logistics networks, and payment systems, while simultaneously embedding its technological standards within that infrastructure. Regarding fintech, through cooperation agreements with Turkish fintech firms and banks, Alibaba has rolled out its payment system in Türkiye, integrating the Turkish payment infrastructure into its global network. China's presence in the economic dimension of the digital sector is underscored by Chinese firms' commitment to further invest in and expand data infrastructure and logistics networks to support operations.

Both when it comes to cloud computing and smart-city technologies, the Chinese engagement is as wide-ranging and multifaceted as in the previous areas. Regarding cloud computing, Chinese stakeholders have managed to embed their tech stack, the set of technologies and software used to build and run systems, into Turkish firms' core infrastructure through far-reaching cooperation agreements and partnerships, which often enable localised Chinese operations without independent corporate presence in Türkiye. The more the e-commerce sector grows, the more cloud penetration deepens and the need for data storage increases. Large Turkish firms have started to build their entire digital stack on a Chinese cloud and store their data in Chinese-operated data centres. Moreover, Sino-Turkish development partnerships for AI-supported operations pave the way for key public

institutions and state agencies to base their digital infrastructure on the architecture of Chinese firms in the future.

Multiple examples of Chinese engagement are relevant for smart-city infrastructure. When it comes to the smart city sector as a whole, however, Chinese involvement shows signs of evolving from collaborating in Türkiye's urban development initiatives to shaping and designing the country's urban-connectivity stack. China's extensive engagement with infrastructure and investment in R&D complements this process, as smart cities require both core platforms and urban applications. Apart from supplying off-the-shelf surveillance-equipment to multiple Turkish sectors, which embeds Chinese systems in Türkiye's public and commercial surveillance networks, Chinese firms have gone as far as signing technology transfer deals in the field of defence and border security with Turkish counterparts. This incorporates Chinese hardware and software directly into Turkish security platforms, which usually handle sensitive data and operate in critical sectors.

All in all, the survey conducted for the needs of this study shows considerable, multi-layered, and firm Chinese presence in Türkiye's digital ecosystem, thus reflecting an established foothold. The Chinese engagement provides Türkiye with the chance to strengthen its capabilities in information technology, AI, and smart manufacturing; areas that are vital for modernizing the country's industrial sector. Moreover, the extensive R&D cooperation, alongside the modest yet existing technology-transfer activities, could bring about long-term advancements, reinforcing Türkiye's role as a regional technology hub. Chinese-owned technology and Chinese firm presence in a country's digital domain do not inherently pose a threat. Yet, this study's underlying theoretical assumption is that Chinese entrenchment in a country's digital domain enables Chinese companies to influence sectors beyond their immediate area of operation and thus give China leverage to engage in activities of weaponisation. Thus, reflections on the risks associated with China's foothold in Türkiye's information technology and digital infrastructure follow below.

4 Risks associated with China's foothold in Türkiye's digital ecosystem

While Chinese engagement with Türkiye's digital ecosystem presents commercial opportunities, it also entails certain security risks. Drawing from Moran and Oldenski's work (see Section 1.3.2), the first threat is that a Chinese acquisition or engagement with a company in Türkiye could enable infiltration, surveillance, or sabotage. The second is the leakage of technology or expertise to a China-controlled entity, potentially harming Türkiye's national interests. The third is creating dependency on a Chinese supplier for critical goods or services.[172] The survey of Chinese engagement in Türkiye's digital ecosystem points to effects spanning all three categories of threat. Türkiye may not perceive these as threats, due to its current close relations with China, but they are nevertheless relevant in the context of Türkiye being a NATO member and in a long-term perspective in which relations with China may worsen. This was the case for Germany, whose relations with Russia deteriorated after 2022, turning its energy dependence on Moscow into a real vulnerability.

Regarding infrastructure, for instance in the example of Netaş localising ZTE's solutions, Turkish carriers enable ZTE-based infrastructure with Turkish-built hardware. This gives the perception of local ownership while the technological core, including firmware, operating systems, and network management, remains Chinese. Integration of software and network management tools into the telecom backbone could expose sensitive government, corporate, and citizen data to interception or remote access, should Beijing seek to weaponise its companies' entrenchment. Turkish legislation that governs the telecom sector includes data localisation requirements and stipulates that critical information and data are stored in Türkiye and remain under Turkish jurisdiction.[173] While the various laws clearly regulate where data are stored and who processes them, they are less explicit regarding the ownership and governance of the underlying hardware and software. This creates a potential loophole through which Chinese business involvement could gain access or exert influence.

Chinese network equipment could also come with hidden vulnerabilities or back-doors, i.e., embedded ways to bypass normal authentication and access controls in

[172] Moran, Oldenski, 2013, p. 55.

[173] See, for instance, Law no 5809 on Electronic Communications, Article 51. Also see the Regulation on Processing of Personal Data and Protection of Privacy in the Electronic Communications Sector, Article 5(2). See even the Presidential Circular on Information and Communication Security Measures 2019/12. The law that governs overall personal data processing, storage, and transfer abroad is Law No 6698 on the Protection of Personal Data.

a network. In fact, backdoors have been detected in ZTE devices in other countries.[174] Telecom core networks handle all traffic, ranging from government, military, and corporate to private conversations. If a backdoor exists, then it could be used for panopticon operations, such as mass surveillance, monitoring specific individuals, or traffic mapping, or even for chokepoint operations, such as disturbing parts of the network or cutting off some targets from network flows (see Section 1.3.2). Thus, this example regarding ZTE's engagement in Türkiye falls within Moran and Oldenski's first and second categories of threats.

Similar risks regarding data interception and disruption of communications on a large scale are associated with the 5G sector. The example of Türk Telekom deploying ZTE's 5G-A ISAC solution and integrating it into its live network to track maritime vessels in real time points to the first and the second categories of threats, that is the potential for infiltration, surveillance, and sabotage as well as the leakage of technology or expertise. The large Chinese investments in developing Türkiye's 5G network overall, however, along with the commitment to provide update services, points to future dependencies and thus fits the description of the third category of threat too, which concerns dependency. Adopting Chinese 5G infrastructure creates a reliance on Chinese technology, maintenance, upgrades, and compatibility. As Türkiye's 5G network will, even partially, depend on Chinese hardware and software, any disruption, manipulation, or weaponisation of the supply chain could affect the country's telecom operations as a whole. Even if Chinese equipment is initially delivered without vulnerabilities or backdoors, new code could be introduced later, for instance during maintenance operations, creating a vulnerability ready to be exploited if political or diplomatic relations between Türkiye and China worsen or if China seeks to indirectly target other Western countries with a presence in Türkiye's digital sphere. Generally, this influence over internet infrastructure and telecom can enable the manipulation of digital platforms with the aim of censoring, spreading disinformation campaigns, suppressing dissenting voices, amplifying polarising content, and shaping opinion in favour of Chinese interests.[175]

Chinese engagement with Türkiye's e-commerce and cloud sectors, interconnected domains that are expanding in parallel (see Section 3.2.2), also raises concerns about dependency. The example of the Alibaba Cloud–E Glober partnership demonstrates how key Turkish sectors become technically and operationally dependent on Chinese cloud architecture. This dependency will likely be prolonged, as the switching costs for moving cloud services elsewhere are high, leading to long-term technological lock-ins. At the same time, the weaponisation of Chinese influence in the e-commerce sector as such could have considerable

[174] See, for instance, Botton, Nicolas, Lee-Makiyama, Hosuk (2018). *5G and national security after Australia's telecom sector security review.* ECIPE Policy Brief, No. 8; Lee, Michael (2012). "Backdoor found in ZTE Android phones," *ZDNet*, 14 May.
[175] Raymond, 2023.

economic effects for Türkiye, especially considering the rising share that e-commerce is taking in total retail sales. Moreover, China's entrenchment in Türkiye's e-commerce sector allows it to embed its technological standards in Türkiye's cloud computing, AI recommendation engines, digital payments, and supporting logistics systems. In addition to technological dependencies, this enables Chinese stakeholders to collect behavioural data, which could be used to exert influence through monitoring users' activities, limiting or restricting access to particular content, and steering users towards other content.[176]

Regarding the cloud sector, independent of the e-commerce sector, the fact that key public and private Turkish institutions are building their digital infrastructure on Huawei's cloud architecture raises serious data-sovereignty concerns. Türkiye's data localisation laws require that sensitive data be stored and processed within Türkiye, aiming to ensure jurisdiction over them and prevent foreign access.[177] As long as the data itself remains in the country, the laws do not necessarily forbid foreign companies from owning or operating local data centres. China's National Intelligence Law requires companies to cooperate with intelligence agencies when requested.[178] Huawei is not state-owned, yet under this law, it could be compelled to aid Beijing's intelligence operations by giving access to data hosted on its cloud in Türkiye, without previously seeking the consent of Turkish stakeholders. This could be harmful for Ankara's or, indirectly, its allies' interests. Although it is easier to carry out coordinated influence and sabotage operations through state-owned enterprises, this law enables such operations by leveraging private companies' insights and resources.[179]

Another aspect worth highlighting concerns the potential risks related to the recruitment of Turkish technical experts in critical technology areas, particularly in connection with Chinese R&D centres established in the country. Huawei, for instance, has long leveraged international talent through its network of research centres worldwide. When skilled Turkish engineers or researchers work in Chinese R&D centres, locally developed expertise and know-how, often built through public funding and national projects, can purposefully flow or unwillingly leak to Chinese entities, the latter signalling the second category of threat. This could lead to compromised technological sovereignty and a talent drain, resulting in a domestic shortage of high-level talent in critical sectors.

[176] Ibid. p. 3, 4.

[177] See the provisions for data localisation, for instance, under the Law No 6698 on the Protection of Personal Data or the Law no 5651 on the Regulation of Broadcasts via Internet and Prevention of Crimes Committed through Such Broadcasts.

[178] Article 7, National Intelligence Law of the People's Republic of China (effective 27 June 2017, revised 27 April 2018).

[179] See, for instance, Junerfält, Tobias, Wannheden, Emil (2024). *Manufacturing vulnerabilities: Chinese minerals, Semiconductors and Green Technologies in the EU*. FOI-R--5524--SE. Kista: Swedish Defence Research Agency (FOI).

Smart-city technologies collect, in their turn, extensive amounts of data on citizens' movement, behaviour, and utilities. The integration of Chinese firms' hardware and software in Türkiye's critical urban infrastructure therefore raises multiple cyber-security and espionage risks. For instance, breaches in smart-city systems could derail essential services such as water supply, or gather intelligence on emergency responses. The fact that Huawei has moved from a partner to an architect of Türkiye's urban connectivity stack deepens the firm's oversight and influence potential even further.

That Chinese technology has crept into Türkiye's critical security space became evident after examining the country's SIS sector. The example of the technology transfer deal between Chinese company Dahua and Turkish firm ASİSGUARD for the co-development of thermal surveillance systems and high-tech cameras for public security, suggests that a surveillance vulnerability could be built into the co-produced systems. Dahua products have a documented history of cybersecurity issues.[180] The fact that the systems are produced locally in Türkiye does not fully mitigate risks, as the technology base or the toolchain could still be based on Chinese design. If compromised, the systems could be remotely accessed, data could be intercepted, and the network could be attacked. Considering that ASİSGUARD operates within defence and border security, this vulnerability is being built within a critical sector for Türkiye's national security. Chinese oversight or control over such key nodes could, by extension, compromise NATO resilience and interoperability, for instance by indirectly degrading command-and-control functions that rely on Turkish systems. This example therefore falls under the first and the second categories of threats, entailing the potential for infiltration, surveillance, or sabotage as well as the potential for leaking technology or expertise to China.

The detection of such vulnerabilities or backdoors by the Turkish authorities could have negative consequences for Sino-Turkish relations, jeopardising the economic benefits of the growing Chinese engagement in the Turkish market and of developing Türkiye's technical capabilities. These risks and built-in vulnerabilities have, however, broader geopolitical and alliance implications.

NATO and the EU share a common interest in preventing disruptions to critical infrastructure, and steps have been taken to increase NATO–EU cooperation on resilience.[181] The resilience of a NATO state's critical infrastructure, however, is

[180] For vulnerabilities related to critical remote code execution, see, for instance, *Bitdefender* (2025). "Vulnerabilities Identified in Dahua Hero C1 Smart Cameras," 30 January; Williams, Wayne (2025). "Hackers could take over millions of Dahua CCTV cameras because of two critical flaws—Here's how to stay safe," *Tech Radar*, 14 August. For authentication bypass, see, for example, Toulas, Bill (2021). "Unpatched Dahua cams vulnerable to unauthenticated remote access," *Bleeping Computer*, 7 October. For botnet infections, see, for instance, Roberts, Paul (2016). "The Hacked Camera Botnet: Not New, Just Big," *The Security Ledger*, 30 September.

[181] As for instance, the establishment of the NATO-EU task force on the resilience of critical infrastructure in 2023.

primarily a national responsibility. Since 2017, NATO's collective resilience planning has been guided by the alliance's seven baseline requirements.[182] Though effective for political-military decision-making, the baselines do not define which entities in a country's infrastructure are critical, how to assess when a disruption becomes significant or how to measure the cascading impacts across sectors.[183] Their value for national operators and regulators is thus limited. Among NATO members, there is no unified position on crucial issues like investment screening, which is vital for the resilience of critical infrastructure, nor a regulatory framework, for instance regarding the use of 5G. Even if there were consensus among the allies, NATO itself is not a regulatory body.

The EU has regulatory power and its Critical Entities Resilience Directive, alongside other complementary directives, fill much of the NATO-baselines' gap.[184] However, the EU does not mandate bans, and leaves decision-making and enforcement of screening mechanisms up to national governments. In the digital sector, the EU has adopted strategies aimed at de-risking rather than decoupling relations with China.[185] Moreover, despite the EU's evolving regulatory framework on direct investment, mechanisms for scrutinising other channels of Chinese access to critical infrastructure beyond direct investment remain limited.[186] This allows room for manoeuvre for both EU member states, and for countries like Türkiye, which are part of some Western institutions yet are not necessarily constrained by them. In every case, Chinese engagement with Türkiye's digital ecosystem could soon raise significant interoperability and trust concerns in both Brussels and Washington, related to hybrid tactics such as cyber intrusions, espionage, and technology infiltration, which use Türkiye as a base while targeting other Western allies or, potentially, alliance cohesion.[187] The timing is particularly sensitive, as Türkiye's role in European defence is currently being strengthened in light of unpredictable American support for Ukraine and a reduced American presence in the Middle East.[188]

---

[182] Those include continuity of government, resilient energy supplies, management of uncontrolled population movement, food and water security, management of mass-casualties and health crises, civil communication systems and transport resilience. See NATO. Resilience, civil preparedness and Article 3.

[183] Kremidas-Courtney, Chris (2025). "Multiple risks, one toolbox: Harmonising NATO and EU approaches to resilience*", Euro-Atlantic Resilience Journal*, Vol. 3(6), p. 3.

[184] Ibid, p. 2-7.

[185] Brinza, Andreea, Berzina-Cerenkova, Una Aleksandra, Le Corre, Philippe, Seaman, John, Turcsanyi, Richard, Vladisavljev, Stefan (2024). *EU–China relations: De-risking or de-coupling—The future of the EU strategy towards China.* European Parliament, Directorate General for External Policies.

[186] Jüris, Frank (2023). *Security implications of China-owned critical infrastructure in the European Union.* European Parliament, Directorate General for External Policies, p. 9.

[187] See, for instance, Tohk, Tauno (2025). *More than a systemic rival: China as a security challenge for the EU*. International Centre for Defence and Security.

[188] Some examples of Türkiye's strengthened defence ties with the EU are the country's participation in the European Sky Shield Initiative, and projects in naval cooperation with Portugal, ammunition production with Poland, and vehicle supplies to Romania; *TRT World* (2024). "Turkish, Greek defence chiefs sign to join European Sky Shield Initiative," 15 February; Özberk, Tayfun (2024). "Portuguese Navy Awards Türkiye's STM Contract to Build Multirole Logistics Support Ships," *Naval News*, 17 December; *Military*

4.1 Reflections on risks for Sweden

Sweden's national security strategy mentions that China's "totalitarian evolution and geopolitical ambitions are a direct threat to Sweden's national security."[189] The same document states that China's use of its cyber capabilities and its ambition to become a leading power in new technology, have consequences for Sweden's security and competitiveness. Lastly, the document declares that China's military–civil fusion, which means that private Chinese companies share their technology with the military, is another factor that threatens Swedish interests.[190] By extension, Türkiye's potential contributions to China's lead in new technologies and military–civil fusion thus have adverse implications for Sweden as well.

The Swedish national security strategy points out, however, that China is the world's second-largest economy, and mentions the importance of maintaining a dialogue and trade with China in areas that are compatible with Sweden's national security.[191] The dilemma of security concerns versus commercial opportunities in Sweden's interaction with China thus becomes evident in Stockholm's strategic thinking. Sweden sets out to tackle this dilemma by anchoring Sino-Swedish relations in a "European strategy with close transatlantic cooperation."[192] There is, however, both a lack of regulatory tools within the EU, which would bind member states to scrutinise non-EU investment in critical assets or access to critical infrastructure, and, as already mentioned, a lack of consensus within NATO on matters related to critical infrastructure resilience.[193] Although Sweden has taken some steps at a national level to protect its network technologies from Chinese influence, it is possible that Swedish security interests are indirectly affected when an EU member state or another NATO country permit Chinese activity within their critical infrastructure.[194] The risks associated with China's foothold in Türkiye's digital ecosystem are thus relevant for Swedish interests, though mainly indirectly. Hybrid tactics, such as cyber intrusions into Türkiye's networks, could target Sweden via Türkiye. Intelligence gathered through such an intrusion could be weaponised by China itself or by its close partners, such as Russia, if China shares

Defence (2025). "Poland and Türkiye Expand Defence Industry Collaboration with Advanced Ammunition Technology Partnership," 8 November; *Türkiye Today* (2025). "Türkiye's largest armored vehicle export makes first shipment to Romania," 10 June.

[189] Regeringens skrivelse 2023/24:163. Nationell säkerhetsstrategi [Government communication 2023/24:163. National security strategy], p. 12.

[190] Ibid.

[191] Regeringens skrivelse 2023/24:163. Nationell säkerhetsstrategi [Government communication 2023/24:163. National security strategy], p 21.

[192] Ibid.

[193] See, for instance, Jüris, 2023, p. 9–10.

[194] An example of such a measure is the banning of Huawei and Huawei products from Swedish network technologies in 2022. See Library of Congress (2022). Sweden: Prohibition on Huawei Products in Swedish 5G Network Upheld, 24 August.

that intelligence with them.[195] Sweden and Swedish interests become potential targets for Chinese weaponisation tactics through three main facilitating factors.

The first factor is through Sweden's NATO membership, which implies that compromised alliance security also means compromised Swedish security. NATO has built a collective security system with shared information, coordination, and interoperability. If the alliance's security is degraded, then the effects cascade quickly, reducing military effectiveness, increasing vulnerability to surprise or coercion, derailing deterrence, and causing domestic political and economic fallout in its member states.

The second facilitating factor is deepened Swedish–Turkish bilateral cooperation in critical sectors currently in the works. During the process of Sweden's NATO-accession, negotiations between Sweden and Türkiye resulted in a set of agreements, which form the basis for enhanced bilateral security and defence cooperation, provided that there is political will in Stockholm and in Ankara.[196] The Swedish and Turkish Armed Forces are negotiating the framework for bilateral military cooperation, with a view to update and renew a previous agreement from 2012.[197] Areas covered in the earlier agreement included military–technical cooperation, training and exercises, logistics, R&D, and the defence industry. The scope of the latest Turkish draft agreement has remained largely the same, yet with increased interest in intelligence exchange, the cyber domain, and counter-terrorism.[198] Considering the penetration of Chinese companies in Türkiye's digital ecosystem, it is possible that an enhanced Swedish–Turkish cooperation that covers critical sectors could affect Swedish intelligence and security by proxy, especially if Türkiye fails to prevent Chinese access to sensitive data.

The third factor that may facilitate Swedish interests being targeted by Chinese weaponisation processes is the presence of Swedish stakeholders in Türkiye. The Swedish telecom company Ericsson, for instance, has a long-standing presence in Türkiye. Its operations focus mainly on R&D, innovation, and expanding collaboration in telecom technology and infrastructure. A recent example of enhanced collaboration between Ericsson and Turkish stakeholders is the Ericsson–Türk Telekom agreement to advance research on transportation safety using 6G technology.[199] Another example is the Ericsson–Turkcell partnership, which supports digital transformation in Türkiye. That includes, for instance, the integration of Ericsson's mediation platform into Turkcell's systems with a view to

[195] For the evolving security cooperation between China and Russia, see for instance, Hsiung, Weidacher, Christopher (2021). *China's evolving security alignment with Russia—Content, motivations and future prospects.* FOI Memo 7540. Kista: Swedish Defence Research Agency (FOI).
[196] See Serveta, 2025.
[197] Ibid, p. 54.
[198] Ibid.
[199] Ericsson (2025). "Ericsson and Türk Telekom forge strategic 6G collaboration," 4 March.

enhance network performance and support data growth.[200] It further includes the deployment of Ericsson's Cloud RAN technology on Turkcell's network, aiming to enable quicker rollout of next-generation services.[201] Moreover, it entails an agreement to jointly develop, deploy, and adopt generative AI solutions across Turkcell's networks and applications.[202] Considering the entrenchment of Chinese companies within Türkiye's main telecom operators and their networks, it cannot be ruled out that China could interfere with Ericsson's systems.

Apart from the security dimension, Chinese stakeholders' increased influence in Türkiye's digital ecosystem also poses competitive challenges to Swedish companies. That becomes particularly evident when considering the cautious but ongoing expansion of Swedish business activities in Türkiye.[203] There are 107 Swedish companies currently operating in Türkiye, of which 17 are active in areas relevant to Türkiye's digital ecosystem.[204] Swedish cybersecurity firms, software and IT companies, as well as providers of security communications and IoT technologies, are likely to face competitive pressures and integration challenges due to expansive Chinese-backed alternatives and Chinese influence with an increasing capability to shape the Turkish government's procurement preferences. The overall risk landscape associated with China's foothold in Türkiye's digital ecosystem is multifaceted and complex. Due to the deepened Sino-Turkish ties, it is hard to assess what kind of data Türkiye willingly shares with China. Assuming that China would not risk targeting or exposing Türkiye to risks, due to the countries' evolving bilateral ties, also assumes that the political relationship between the countries will be stable over time. Reality is more complex than that. Even if China would not target Türkiye itself, and provided that Beijing has an interest in carrying out activities of weaponisation, it could judge that risking its bilateral relation with Türkiye is not as valuable as targeting and degrading NATO security. Thus, it could use Türkiye as a base for targeting Western allies or NATO as a whole. That makes the Chinese foothold in the Turkish digital ecosystem, an ecosystem that is, in practice, transnational and embedded within broader technological networks, a matter of utmost relevance for Türkiye's allies in the West, including Sweden.

[200] Ericsson (2023). "Turkcell modernizes the Ericsson Mediation platform to meet growing technology demands," 16 January.
[201] Ericsson (2024). "Ericsson and Turkcell strengthen partnership with 5G Cloud RAN trial deployment," 16 August.
[202] Ericsson (2025). "Ericsson and Turkcell collaborate at MWC25 to advance Generative AI solutions in Türkiye," 4 March.
[203] Business Sweden (2024). Business climate survey for Swedish companies in Türkiye 2024.
[204] Data obtained via email correspondence with Business Sweden representative, 6 September 2025.

5 Suggestions for future research

Both this study's delimitations and findings point to several areas that warrant further investigation.

Electrical power is fundamental for the operation of data centres, communication networks, and other digital infrastructure. Energy can also be weaponised, for example by freezing digital infrastructure. Further work is therefore needed to examine China's role in Türkiye's energy sector in general, and power grids in particular. Smart grids are modern, digitally enhanced electricity networks that use sensors, automation, and communication technology to manage electricity flows. Smart grids are linked to ICT, smart city technology, and the DSR. Further research into this sector would help provide a more comprehensive view, complementing the present study's inquiry.

FOI currently analyses various paths that Chinese outward direct investment takes on its journey toward the ultimate destination, one such path being transiting through one or several intermediate jurisdictions. Since Türkiye welcomes Chinese investment, the volume of investment routed via foreign jurisdictions need not be large. However, to provide a fuller picture of Chinese engagement, such an inquiry would be beneficial for Türkiye as well.

While the present study did not examine social media, there are nonetheless compelling examples of Chinese presence in this sector. As of early 2025, Türkiye's population is estimated at 87.7 million. Meanwhile, TikTok has around 37.7 million users in Türkiye, with a penetration rate of approximately 62%.[205] This means that 62% of the people eligible or likely to use TikTok are active users of the platform. This is high compared to other European countries, where penetration rates usually range between 30% and 50%. Further research into this area would complement the insights gained from this study about the digital sector.

A relevant aspect is the prevalence of Chinese smartphones in Türkiye. Examining this, alongside the adoption of Chinese standards and potential risks of data manipulation or leakage, would further enrich the understanding of China's foothold in Türkiye's digital ecosystem.

This study did not examine China as an actor, which would involve analysing Beijing's decision-making processes and considering the benefits it seeks to gain from engaging with Türkiye, in particular, or leveraging its foothold in sensitive sectors in the country. Further in-depth exploration of the role that NATO member Türkiye plays in Beijing's calculations remains an opportunity for future research.

[205] Kemp, Simon (2024). "Digital 2024: Turkey", *DataReportal*, 23 February; Ceci, Laura (2025). "TikTok penetration in selected countries and territories as of February 2025", *Statista*, 10 February.

References

AEI (2024). China Global Investment Tracker. “Chinese investments and contracts in Turkey (2005–2024).”

Akcay, Nurettin (2021). “Amid tensions with Turkey, China is putting the Kurdish issue in play,” *The Diplomat,* 4 December.

Al Arabiya English (2023). “Alibaba plans $1bln logistics hub at Istanbul airport, data centre near Ankara,” 8 January.

Alalouff, Ron (2018). “The spectacular rise of the Chinese video surveillance industry,” *IfsecGlobal,* 7 March.

Alemdaroğlu, Ayça, Tepe, Sultan (2023). “Turkey’s strategic partneship with China: A feminist recount” In Özkeçeçi-Taner, Binnur, Açıkmeşe, Sinem (2023). *One hundred years of Turkish foreign policy (1923–2023): Historical and theoretical reflections*. Cham: Palgrave MacMillan.

Alhosban, Amal, Pesingu, Saichand, Kalyanam, Krishnaveni (2024). “CVL: A cloud vendor lock-in prediction framework,” *Mathematics,* Vol. 12(3), 387, p. 1–18.

Alibaba Cloud (2018). “Alibaba Clouds expands into Turkey,” 9 April.

Almén, Oscar, Carlsson, Hanna (2025). *The Chinese Communist Party’s influence over businesses*. FOI-R--5695--SE.

Aluf, Dale (2023). “China’s digital footprint grows in the Middle East and North Africa,” *Mapping Global China*, 8 June.

Anadolu Agency (2024). “Türkiye–China meeting to foster regional, global peace and prosperity,” 8 November.

Anadolu Agency (2016). “Chinese *ZTE* buys stake in Turkey’s Netas for $101M,” 6 December.

Anas, Omair (2022). *Turkey's Asia Relations.* London: Palgrave Macmillan.

ANews (2018). “Turkcell, Huawei sign deal on smart cities in Turkey,” 24 October.

ASISGUARD (2025). About us.

AsMag (2010). “Hikvision Upgrades Turkish Ziraat Bank Surveillance Systems,” 28 January.

Atlı, Altay (2024). “Çin’in Türkiye’ye dev yatırımı hangi kapıları açabilir?” [What doors could China’s massive investment in Turkey open?], *Fikir Turu,* 6 August.

Attarwala, Fatima (2023). “Alibaba expands international business with 2 billion investment in Turkey’s Trendyol,” *Investopedia*, 18 September.

Autio, Erkko, Komlósi, Éva, Szerb, Laszlo, Tiszberger, Monika, Park, Donghyun, Jinjarak, Yothin (2024). “Digital entrepreneurship landscapes in developing

Asia: Insights from the Global Index of Digital Entrepreneurship Systems (GIDES)," ADB Economics Working Paper Series, No. 720. Asian Development Bank.

Aydın, Erdal, Kılınç, Savrul, Burcu (2014). "The relationship between globalization and e-commerce: Turkish case," *Procedia—Social and Behavioural Sciences*, Vol. 150, p.1267-1276.

Balzacq, Thierry, Leonard, Sarah, Ruzicka, Jan (2015). "Securitization revisited: Theory and cases," *International Relations,* Vol. 30(4), p. 494–531.

Bazaar Times (2022). "Technology brand Vivo continues to invest in Türkiye," 15 December.

BBC News Türkçe (2022). "Erdoğan: Hedef Şanghay İşbirliği Örgütü üyeliği" [Erdoğan: The goal is membership in Shanghai Cooperation Organisation], 17 September.

Bitdefender (2025). "Vulnerabilities Identified in Dahua Hero C1 Smart Cameras," 30 January.

Bloomberg HT (2019). "Ödeme platformu ininal, Alipay'in Türkiye'deki ilk iş ortağı oldu" [The payment platform ininal became Alipay's first partner in Türkiye], 21 May.

Botton, Nicolas, Lee-Makiyama, Hosuk (2018). *5G and national security after Australia's telecom sector security review.* ECIPE Policy Brief, No. 8.

Brinza, Andreea, Berzina-Cerenkova, Una Aleksandra, Le Corre, Philippe, Seaman, John, Turcsanyi, Richard, Vladisavljev, Stefan (2024). *EU–China relations: De-risking or de-coupling – The future of the EU strategy towards China*. European Parliament, Directorate General for External Policies.

Brown, Scott (2024). "Beyond the great firewall: EU and US responses to the China challenge in the global digital economy," *Journal of European Integration*, Vol. 46(7), p. 1089–1110.

Business Sweden (2024). Business climate survey for Swedish companies in Türkiye 2024.

Camba, Alvin (2020). "The Sino-centric capital export regime: State-backed and flexible capital in the Philippines," *Development and Change,* Vol. 51(4), p. 970–997.

Caragliu, Andrea, Del Bo, Chiara, Nijkamp, Peter (2011). "Smart cities in Europe," *Journal of Urban Technology*, Vol. 18(2), p. 65–82.

Ceci, Laura (2025). "TikTok penetration in selected countries and territories as of February 2025", *Statista*, 10 February.

Celik Gözde (2020). "WeChat Pay launches service in Turkey targeting Chinese tourists," *KrAsia*, 29 July.

Cheng, Jing, Zeng, Jinghan (2023). “Digital Silk Road as a slogan instead of a grand strategy,” *Journal of Contemporary China*, Vol. 33(149), p. 823–838.

Choudary, Sangeet, Paul (2020). “China’s country-as-platform strategy for global influence,” *Brookings*, 19 November.

Cong, Wanshu (2024). “The Spatial Expansion of China’s Digital Sovereignty: Extraterritoriality and Geopolitics” In Jiang Min, Belli Luca (2024). *Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance*. Cambridge: Cambridge University Press.

Creemers, Rogier, Dorwart, Hunter, Neville, Kevin, Schaefer, Kendra (2022). *Translation: 14th five-year plan for national informalization*. DigiChina, Cyber Policy Center, Freeman Spogli Institute.

Çamlıbel, Cansu (2014). “Turkey ‘cannot ignore’ Western concerns over missile deal,” *Hürriyet English*, 18 February.

Çolakoğlu, Şelcuk (2021). *Turkey’s Policy towards Taiwan: From Cross-Strait Relations to Syrian Refugees.* Global Taiwan Institute, 13 January.

Çolakoğlu, Selçuk (2018). “Turkey–China Relations: From strategic cooperation to strategic partnership,” Middle East Institute, 20 March.

Çolakoğlu, Selçuk (2015). “Dynamics of Sino-Turkish relations: A Turkish perspective,” *East Asia*, Vol. 32, p. 21.

Çolakoğlu, Selçuk (2013). “Sino-Turkish Relations: Assessments & Shortcomings,” *China Policy Institute*, 1 October.

Çolakoğlu, Selçuk (2012). “Turkey’s East Asian Policy: From security concerns to trade partnerships,” *Perceptions*, Vol. 17(4), s. 129–158.

Daily Sabah (2025). “Türkiye's e-commerce volume reached $90B in 2024: Trade minister,” 6 May.

Daily Sabah (2021). “China’s Techno Mobile starts production at Turkey factory,” 24 May.

Daily Sabah (2021). “Alibaba invests $350M in capital increase to Turkey’s Trendyol,” 21 April.

Daily Sabah (2021). “Chinese Xiaomi to begin smartphone production in Turkey,” 4 February.

Daily Sabah (2019). “Turkey’s İş Bank, China's AliPay expand cooperation on payment systems,” 25 December.

Daily Sabah (2019). “Turkey, Huawei sign cooperation protocol on R&D for smart cities,” 29 March.

Data Center Knowledge (2023). “Bloomberg News: Alibaba Plans logistics hub at Istanbul airport, data centre near Ankara,” 9 January.

Du, Julan, Zhang, Yifei (2018). "Does one Belt one Road Initiative promote Chinese overseas direct investment?" *China Economic Review,* Vol. 47, p. 189–205.

Dutta, Soumitra, Lanvin, Bruno (2022). *The Network Readiness Index 2022.* Portulans Institute.

Dünya (2024). "IBT Solar dünyanın 1 numaralı batarya üreticisi CATL ile işbirliği yapıyor" [IBT Solar Collaborates with the World's Number One Battery Manufacturer CATL], 27 May.

Egeli, Sıtkı (2019). "Making sense of Turkey's Air and Missile Defense Merry-go-round," *All Azimuth,* Vol. 8(1), p. 69–92.

El Kadi, Tin Hinane (2025). *Local agency is shaping China's digital footprint in the Gulf.* Carnegie Endowment, 6 January.

Ericsson (2025). "Ericsson and Türk Telekom forge strategic 6G collaboration," 4 March.

Ericsson (2025). "Ericsson and Turkcell collaborate at MWC25 to advance Generative AI solutions in Türkiye," 4 March.

Ericsson (2024). "Ericsson and Turkcell strengthen partnership with 5G Cloud RAN trial deployment," 16 August.

Ericsson (2023). "Turkcell modernizes the Ericsson Mediation platform to meet growing technology demands," 16 January.

Erie, Matthew, Streinz, Thomas (2021). "The Beijing effect: China's Digital Silk Road as transnational data governance," *New York University of International Law and Politics,* Vol. 54(1), p. 1–92.

Esen, Berk, Gumuscu, Sebnem (2020). "Why did Turkish democracy collapse? A political economy account of AKP's authoritarianism," *Party Politics,* Vol. 27(6), p. 1075–1091.

Eurasia Group (2020). *The Digital Silk Road: Expanding China's digital footprint.* Fudan University.

European Commission (2020). I-DESI 2020: How digital is Europe compared to other major world economies?, 17 December.

Farrell, Henry, Newman, Abraham (2019). "Weaponized interdependence: How global economic networks shape state coercion," *International Security,* Vol. 44(1), p. 42–79.

Finextra (2024). "İşbank expands partnership with Alipay+," 20 December.

Gençoğlu Onbaşi, Funda (2016). "Gezi Park protests in Turkey: from 'enough is enough' to counter-hegemony?" *Turkish Studies,* Vol. 17(2), p. 272–294.

Global Times (2023). "Turkey–China business conference announced to strengthen cooperation in digital transformation," 13 July.

Gomber, Peter, Koch, Jascha-Alexander, Siering, Michael (2017). “Digital finance and FinTech: Current research and future research directions,” *Journal of Business Economics*, Vol. 87, p. 537–580.

Gordon, David, Nouwens Meia (2020). “Introduction,” in Gordon, David, Nouwens Meia (2020). “The Digital Silk Road: China’s Technological Rise and the Geopolitics of Cyberspace,” *Adelphi Series,* Vol. 60(487–489).

Gostoli, Ylenia (2025). “Turkey’s AI-powered protest crackdown,” *New Lines Magazine*, 5 June.

Guliyev, Vusal (2024). “Turkish–Chinese rapprochement: Growing Chinese investment in Turkiye,” *Caspian–Alpine Society,* 3 December.

Geybullayeva, Arzu (2025). “In Turkey, a controversial law on cybersecurity is widely seen as yet another censorship tool,” *Global Voices,* 27 March.

Gürel, Burak, Kozluca, Mina (2022). “Chinese investment in Turkey: The Belt and Road Initiative, rising expectations and ground realities,” *European Review*, Vol. 30(6), p. 806–834.

Hacaoğlu, Selcan, Kozok, Firat (2024). “Turkey Bids to Join BRICS in Push to Build Alliances Beyond West,” *Bloomberg*, 2 September.

He, Laura (2024). “Chinese EV giant BYD to build $1 billion plant in Turkey,” *CNN*, 9 July.

He, Yujia. (2024). “Chinese digital platform companies’ expansion in the belt and road countries,” *The Information Society*, Vol. 40(2), p. 96–119.

Hemmings, John (2017). *Safeguarding our systems: Managing Chinese investment into the UK’s digital and critical national infrastructure.* The Henry Jackson Society.

Hikvision (2020). Ankara Metro Mall Surveillance Project.

Hikvision (2020). “Hikvision: securing one of the busiest shopping malls in Turkey’s capital,” 1 September.

Hsiung, Weidacher, Christopher (2021). *China’s evolving security alignment with Russia – Content, motivations and future prospects*. FOI Memo 7540. Kista: Swedish Defence Research Agency (FOI).

Huawei (2025). Turkey Research and Development Center.

Huawei (2025). “Turkcell and Huawei Sign Memorandum of Understanding for Leading Network Joint Innovations at MWC 2025,” 4 March.

Huawei (2024). “Turkcell and Huawei signed three MOUs on 5.5G, green energies, and AI based networks at MWC 2024,” 29 February.

Huawei (2024). “Türkiye’de daha güçlü bir bulut bilişim ekosistemi için Huawei Cloud ve Logosoft’tan stratejik ortaklık” [Strategic partnership from Huawei Cloud and Logodoft for a stronger cloud computing ecosystem in Turkiye], 22 February.

Huawei (2022). “Huge collaboration in 5G from Türk Telekom and Huawei,” 12 March.

Huawei (2019). “Turkcell Joins Hands with Huawei to Build a 5G-oriented All-Cloud Core Network,” 15 February.

Huawei (2017). “Huawei and Vodafone Turkey Sign the TechCity 2.0 MoU,” 9 June.

Huawei Cloud (2024). “Hepsiburada Aims to Enhance Efficiency by Optimizing Costs with Huawei Cloud,” 18 October.

Huawei Cloud (2024). “Huawei Cloud Unveils AI-Native Cloud, Becoming the Preferred Cloud of Turkish Leading Enterprises,” 10 October.

Huaxia (2023). “China’s tech giant Huawei launches localized cloud in Türkiye,” 13 July.

Hussain, Ejaz (2022). “The Belt and Road Initiative, the Middle Corridor and Turkey’s Asia Policy: An Analysis” in Anas, Omair (2022). *Turkey's Asia Relations.* London: Palgrave Macmillan.

International Trade Centre. Bilateral trade between China and Türkiye in 2024. Product: All products.

International Telecommunications Union (2024). *Measuring digital development: The ICT Development Index 2024*. ITU Publications.

Ismagilova, Elvira, Hughes, Laurie, Rana, Nripendra, Dwivendi, Yogesh (2022). “Security, privacy and risks within Smart Cities: Literature review and development of a Smart City interaction framework,” *Information Systems Frontier,* Vol. 24, p. 393–414.

Jia, Lianrui, Winseck, Dwayne (2018). “The political economy of Chinese internet companies: Financialization, concentration, and capitalization,” *International Communication Gazette*, Vol. 80(1), p. 30–59.

Jiang, Min, Belli, Luca (2024). *Digital sovereignty in the BRICS countries. How the Global South and emerging power alliances are reshaping digital governance.* Cambridge: Cambridge University Press.

Jüris, Frank (2023). *Security implications of China-owned critical infrastructure in the European Union.* European Parliament, Directorate General for External Policies.

Kamu Ihale Kurulu Kararlarıç 2019/323197 İhale Kayıt Numaralı “Afyonkarahisar İl Emniyet Müdürlüğü ve Farklı Lokasyonlardaki Çevre Güvenlik Kamera Sistemi Yapım İşi” İhalesi - Tarih: 24.10.2019 - No: 2019/UY.II-1380, [Public Procurement Board Decisions. Tender Registration Number 2019/323197 “Afyonkarahisar Provincial Police Department and Perimeter Security Camera System Construction Work in Different Locations” - Date: 24.10.2019 - No: 2019/UY.II-1380].

Kasapoğlu, Can (2019). “Türkiye'nin balistik füze teknolojisinde yeni aşama” [A new step in Turkey’s ballistic missile technology], *Anadolu Ajancı*, 26 June.

Katz, Raul, Callorda, Fernando (2018). "Accelerating the development of Latin American digital ecosystem and implications for broadband policy, *Telecommunications Policy,* Vol. 42(9),p. 661–681.

Kemp, Simon (2024). “Digital 2024: Turkey”, *DataReportal*, 23 February.

Khatib, Mutamed, Salman, Nael (2018). *Mobile computing—Technology and applications*. InTech.

Kleinhans, Jan-Peter, Rühlig, Tim (2024). “Introduction: Reverse dependencies on China,” in Rühlig, Tim (2024). *Reverse dependency: Making Europe’s digital technological strengths indispensable to China*. Digital Power China Report 3, German Council on Foreign Relations.

Koepp, Robert (2020). “Locating the Digital Silk Road in the Belt and Road Initiative,” in Gordon, David, Nouwens Meia (2020). “The Digital Silk Road: China’s Technological Rise and the Geopolitics of Cyberspace,” *Adelphi Series,* Vol. 60(487–489).

Kremidas-Courtney, Chris (2025). “Multiple risks, one toolbox: Harmonising NATO and EU approaches to resilience”, *Euro-Atlantic Resilience Journal,* Vol. 3(6).

Kunt, Rasim, Anil (2019). “Asisguard İle Dahua Teknoloji’den kamu güvenliği adına önemli anlaşma” [Important Agreement for Public Security Between Asisguard and Dahua Technology], *DefenceTurk,* 1 May.

Lagiewska, Magdalena (2024). “Legal aspects of the Digital Silk Road: Trends and Challenges,” in Sahakyan, Mher (2024). *Routledge Handbook of Chinese and Eurasian International Relations.* London: Routledge.

Lee, Michael (2012). “Backdoor found in ZTE Android phones,” *ZDNet,* 14 May.

Library of Congress (2022). Sweden: Prohibition on Huawei Products in Swedish 5G Network Upheld, 24 August.

Mahfoud, Ayşe, Tecimer, Cem (2022). “The Turkish technology ecosystem: An introduction,” *Norton Rose Fulbright,* 15 June.

Makowska, Marta (2024*). China's digital authoritarianism vs EU technological sovereignty: The impact on Central and Eastern Europe*. Council on Foreign Relations.

Mazzucato, Mariana, Shipman, Alan (2014). "Accounting for productive investment and value creation," *Industrial and Corporate Change,* Vol. 23(4), p. 1059–1085.

Milhaupt, Curtis, Lin, Lauren, Yu-Hsin (2023). *Can Chinese firms be truly private?*. CSIS, Big Data China, 7 February.

Milhaupt, Curtis, Zheng, Wentong (2015). "Beyond Ownership: State Capitalism and the Chinese Firm," *Georgetown Law Journal*, Vol. 103, p 665–722.

Military Defence (2025). "Poland and Türkiye Expand Defence Industry Collaboration with Advanced Ammunition Technology Partnership," 8 November.

Millitet (1996). "Çinle gizli füze anlaşması" [Secret missile deal with China], 20 December; Weitz, Richard (2010). "Turkey and China establish strategic partnership," *The Turkey Analyst,* 25 October.

Mobile World Live (2025). "Türk Telekom and ZTE complete the world's first 1.6T with 12THz bandwidth DWDM trial on a live network," 4 April.

Mobile World Live (2022). "ZTE assists Turk Telekom in core sites expansion of 100G&B100G metro optical network," 5 July.

Moran, Theodore, Oldenski, Lindsay (2013). *Foreign direct investment in the United States: Benefits, suspicions and risks with special attention to FDI from China.* Peterson Institute for International Economics.

MSoftserv (2025). "Difference between cloud computing and data centre?" 19 June.

Mügge, Daniel (2023). "The securitization of the EU's digital tech regulation," *Journal of European Public Policy*, Vol. 30(7), p. 1431–1446.

Nagel, Avi (2021). "E-commerce integration in China," *The FinTech Times,* 18 March.

NATO. Resilience, civil preparedness and Article 3.

Netaş (2022). Netaş annual report 2022.

National Intelligence Law of the People's Republic of China (中华人民共和国国家情报法).

Nilgün, Eliküçük Yildirim, Gözde, Yilmaz (2023). "Use/misuse of Chinese BRI investment? BRI-related crony capitalism in Turkey," *Southern European and Black Sea Studies,* Vol. 23(2), p. 365–383.

Nouwens, Meia (2022). *NATO and China: Addressing new challenges.* CSDS Policy Brief.

Nouwens, Meia (2020). ”Identifying the Silk Road,” in Gordon, David, Nouwens Meia (2020). “The Digital Silk Road: China’s Technological Rise and the Geopolitics of Cyberspace,” *Adelphi Series,* Vol. 60(487–489).

NS Energy (2019). “Hunutlu Thermal Power Plant,” 27 September.

OEC (2025). China Trade Data.

Opara-Martins, Justice (2018). “Taxonomy of cloud lock-in challenges” in Khatib, Mutamed, Salman, Nael (2018). *Mobile computing – Technology and applications*. InTech.

OPPO (2021). “Türkiye'deki Fabrikasında Üretime Başlayan OPPO, Global Üretim Kapasitesini Artırdı” [OPPO, which started production in its factory in Turkey, has increased its global production capacity], 12 July.

Osmanlı, Seyda Nur (2024). “Türkiye-Çin İlişkileri: İmkanlar ve zorluklar” [Turkey–China relations: Opportunities and challenges], *Center for Eurasian Studies,* Vol. 19, 22 November.

Öğretmenoğlu, Ozan (2023). “Siro; Togg-Farasis ortaklığından doğan batarya şirketi hakkında bilmeniz gerekenler” [Siro: What You Need to Know About the Battery Company Born from the Togg-Farasis Partnership], *Log*, 24 April.

Öngür, Çandaş (2025). *The US–China Tech war: Where does Turkey stand?.* SWP Comment, No 12. Centre for Applied Turkey Studies.

Özberk, Tayfun (2024). “Portuguese Navy Awards Türkiye’s STM Contract to Build Multirole Logistics Support Ships,” *Naval News,* 17 December.

Özkan, Sedef (2022). “Asisguard 2022’de sınır güvenliğine odaklanıyor” [Asisguard focuses on border security in 2022], *BT Haber*, 4 April.

Özkeçeçi-Taner, Binnur, Açıkmeşe, Sinem (2023). *One hundred years of Turkish foreign policy (1923–2023): Historical and theoretical reflections*. Cham: Palgrave MacMillan.

Özşahin, Mustafa, Donelli, Federico, Gasco, Riccardo (2021). “China–Turkey Relations from the perspective of neoclassical realism,” *Contemporary Review of the Middle East,* Vol. 9(2), p. 218–239.

Pearson, Margaret, Rithmire, Meg, Tsai, Kellee (2021). “Party-state capitalism in China,” *Current History*, p. 207–213.

Presidency of the Republic of Türkiye (2020). Regulation on Processing of Personal Data and Protection of Privacy in the Electronic Communications Sector. Official Gazette No. 31324, 4 December.

Presidency of the Republic of Türkiye (2019). Presidential Circular on Information and Communication Security Measures No. 2019/12.

Presidency of the Republic of Türkiye (2016). Law no 6698 on the Protection of Personal Data. Official Gazette No. 29677, 7 April.

Presidency of the Republic of Türkiye (2008). Law no 5809 on Electronic Communications. Official Gazette No. 27056, 10 November.

Presidency of the Republic of Türkiye (2007). Law no 5651 on the Regulation of Broadcasts via Internet and Prevention of Crimes Committed through Such Broadcasts. Official Gazette No. 26530, 23 May.

Presidency of the Republic of Türkiye. Türkiye's FDI Landscape at a glance 2024.

Presidency of the Republic of Türkiye, Digital Transformation Office. National Artificial Intelligence Strategy 2021–2025.

Presidency of the Republic of Türkiye, Investment and Finance Office. Huawei.

Presidency of the Republic of Türkiye. Investment and Finance Office. Success Stories: Netaş.

Presidency of the Republic of Türkiye, Investment and Finance Office (2024). "Türkiye and China Strengthen Historic Ties for Future Economic Growth at CISCE 2024," 28 November.

President of the Republic of Türkiye, Investment and Finance Office (2024). "Ganfeng Lithium and Yiğit Akü Announce USD 500 Million Battery Investment in Türkiye," 5 September.

Presidency of the Republic of Türkiye, Investment and Finance Office (2015). "Chinese consortium buys into Turkish port with USD 940 million investment," 28 September.

Presidency of the Republic of Türkiye, Ministry of Foreign Affairs. Türkiye's Multilateral Transportation Policy.

Presidency of the Republic of Türkiye, Ministry of Foreign Affairs. Türkiye–People's Republic of China Economic and Trade Relations.

Presidency of the Republic of Türkiye, Presidency of Strategy and Budget. Twelfth development plan (2024–2028).

Primack, Dan (2018). "Scoop: Alibaba paid $750 million for Turkish startup Trendyol," *Axios*, 14 August.

Qiu, Jack, Linchuan, Yu, Peter, Oreglia, Elisa (2022). "A new approach to the geopolitics of Chinese internets," *Information, Communication & Society*, Vol. 25(16), p. 2335–2341.

Ray Haber (2023). "Security Systems are being Renewed at Sabiha Gökçen Airport," 20 October.

Raymond, Peter (2023). "Re-platformed planet? Implications of the rise and spread of Chinese platform technologies," *CSIS*, 29 March.

Regeringens skrivelse 2023/24:163. Nationell säkerhetsstrategi. [Government communication 2023/24:163. National security strategy].

Roberts, Paul (2016). “The Hacked Camera Botnet: Not New, Just Big,” *The Security Ledger*, 30 September.

Rühlig, Tim (2024). *Reverse dependency: Making Europe’s digital technological strengths indispensable to China.* Digital Power China Report 3, German Council on Foreign Relations.

Rühlig, Tim (2020). *Technical standardisation, China and the future international order: A European perspective.* Heinrich Böll Stiftung.

Sahakyan, Mher (2024). *Routledge Handbook of Chinese and Eurasian International Relations.* London: Routledge.

Serveta, Marianna (2025). *Turkiets säkerhetspolitiska färdriktning: Strategisk autonomi och stormaktsberoenden* [Türkiye’s security policy direction: Strategic autonomy and great power dependencies]. FOI-R--5781--SE. Kista: Swedish Defence Research Agency (FOI).

Serveta, Marianna (2024). *Chasing the Red Apple: Turkey’s Quest for Strategic Autonomy.* FOI Memo 8568. Kista: Swedish Defence Research Agency (FOI).

Sezer, Can (2020). ”Turkey’s Turkcell signs deal to use Huawei’s mobile services,” *Reuters*, 12 February.

Sharma, Ray (2022). “ZTE, Turkcell Deploy 'World's First' Commercial 12THz WDM System,” *The Fast Mode*, 6 June.

Silk Road Fund (2023). “Silk Road Fund and the Investment Office of the Presidency of Turkey Co-hosted the Roundtable on China–Turkey Investment Cooperation,” 27 July.

Simon, Luis (2023). “NATO’s China and Indo-Pacific conundrum,” NATO Review, 22 November.

Sönmez, Mustafa (2022). “Turkey’s central bank continues window dressing with currency swaps,” *Al Monitor*, 26 June.

Şimşek, Bariş (2017). “Turkish, Chinese telecom partnership looks to provide technical infrastructure for Belt and Road project.” *Daily Sabah*, 5 December.

T.C. Sanayi ve Teknoloji Bakanlığı. Yabancı Sermayeli Firma Listesi. 30.06.2025 Tarihi itibariyle Türkiye’de faaliyette bulunan yabancı sermayeli firmalar listesi [Republic of Türkiye Ministry of Industry and Technology. List of companies with foreign capital in Turkiye as of the end of June 2025].

Terihoğlu, Merve (2022). *Cronies in crises: Economic woes, Clientelism, and elections in Turkey.* Heinrich Böll Stiftung.

The Brand Age (2015). "Alibaba.com'un Türkiye'deki Yeni İş Ortağı Mehmet Ali Yalçındağ'ın E-Glober'ı Oldu" [Mehmet Ali Yalçındağ's E-Glober becomes Alibaba.com's new business partner in Turkey], 30 November.

The Global Security Market (2013). "Hikvision overcomes terrain to secure Turkish telecom," 29 October.

The Middle Eastern Security Market (2018). "Dahua attracts new business with international roadshows," 22 November.

Tohk, Tauno (2025). *More than a systemic rival: China as a security challenge for the EU.* International Centre for Defence and Security.

Toulas, Bill (2021). "Unpatched Dahua cams vulnerable to unauthenticated remote access," *Bleeping Computer*, 7 October

Türkiye Cumhuriyet Merkez Bankası (2025). "Central Bank of the Republic of Turkiye and People's Bank of China renew bilateral currency swap arrangement," 13 June.

Türkiye Gazetesi (2025). "1 milyar dolarlık hamle! Tarifeler korkuttu, yatırımı öne çektiler" [A 1 billion dollar move! Tariffs caused concern, so they brought the investment forward], 2 July.

Türkiye Today (2025). "Türkiye's largest armored vehicle export makes first shipment to Romania," 10 June.

Triolo, Paul (2020). "The Digital Silk Road and the evolving role of Chinese technology companies," in Gordon, David, Nouwens Meia (2020). "The Digital Silk Road: China's Technological Rise and the Geopolitics of Cyberspace," *Adelphi Series*, Vol. 60(487–489).

TRT World (2024). "Turkish, Greek defence chiefs sign to join European Sky Shield Initiative," 15 February.

Uluyol, Yalkun (2024). *Partnership with limits: China Turkey relations in the late AKP era.* Heinrich Böll Stiftung, 20 March.

Vanberghen, Christina (2025). "How Beijing's digital strategy is reshaping global rules – and what Europe should do about it," *Modern Diplomacy,* 25 May.

Vecchi, Alessandra, Brennan, Louis (2022). "Two tales of internationalization – Chinese internet firms' expansion into the European market," *Journal of Business Research,* Vol. 152, p.106–127.

Wanshu, Cong (2024). "The spatial expansion of China's digital sovereignty: Extraterritoriality and geopolitics" in Jiang, Min, Belli, Luca (2024). *Digital sovereignty in the BRICS countries. How the Global South and emerging power alliances are reshaping digital governance.* Cambridge: Cambridge University Press.

Weitz, Richard (2010). "Turkey and China establish strategic partnership", *The Turkey Analyst,* 25 October.

Williams, Wayne (2025). “Hackers could take over millions of Dahua CCTV cameras because of two critical flaws—here’s how to stay safe,” *Tech Radar*, 14 August.

Wright, Charity (2021). “China’s digital colonization: Espionage and repression along the Digital Silk Road,” *SAIS Review of International Affairs.* Vol. 41(2), p. 89–113.

Xiao, Estelle (2024). “China–Türkiye trade and investment profile,” *ChinaBriefing*, 18 October.

Xintong, Wang, Yutong, Lu (2025). “Chinese Government Takes Over Faltering Battery-Maker Farasis,” *Caixing Global*, 18 April.

Xinhua Net (2017). “Istanbul new airport to use Nuctech-made inspection equipment,” 29 December.

Yeşiltaş, Murat (2020). “Deciphering Turkey’s assertive military and defence strategy: Objectives, pillars and implications,” *Insight Turkey*, Vol. 22(3), p. 89–114.

Yildirim, Goksel, Yildirim, Emir (2025). “Turkish defense industry’s new ‘national eye’ gimbal Aggoz empowers UAVs,” *Anadolu Agency*, 4 March.

Yilmaz, Ihsan, Mamouri, Ali, Morieson, Nicholas, Omer Huhammad (2025). *The Transnational Diffusion of Digital Authoritarianism: From Moscow and Beijing to Ankara*. European Centre for Populism Studies, 12 May.

Yiming, Guo (2017). “Digital economy cooperation to empower Belt, Road,” *China.org*, 4 December.

Yıldırım, Nılgün (2024). *The Uyghur issue in Turkey–China relations.* Heinrich Böll Stiftung, 5 April.

Yımlaz, Emirhan (2024). “Cooperation with Chinese state-owned company beginning of tech, trade base in Türkiye,” *Anadolu Agency*, 10 August.

Zhang, Longmei, Chen, Sally (2019). “China’s digital economy: Opportunities and risks,” *IMF e-library*, 17 January.

ZTE (2025). “Türk Telekom and ZTE launch Europe’s first millimeter-wave supported 5G-A ISAC maritime management solution,” 10 March.

ZTE (2025). “ZTE, Netaş, Turkcell strengthen collaboration with server innovations and localisation efforts,” 21 March.

ZTE (2025). “ZTE and Turkcell sign MoU to drive 5G-A innovation,” 10 March.

ZTE (2024). “Türk Telekom and ZTE conduct Europe-first 3-in-1 50G PON Combo trial in Türkiye” 19 March.

ISSN 1650-1942

www.foi.se