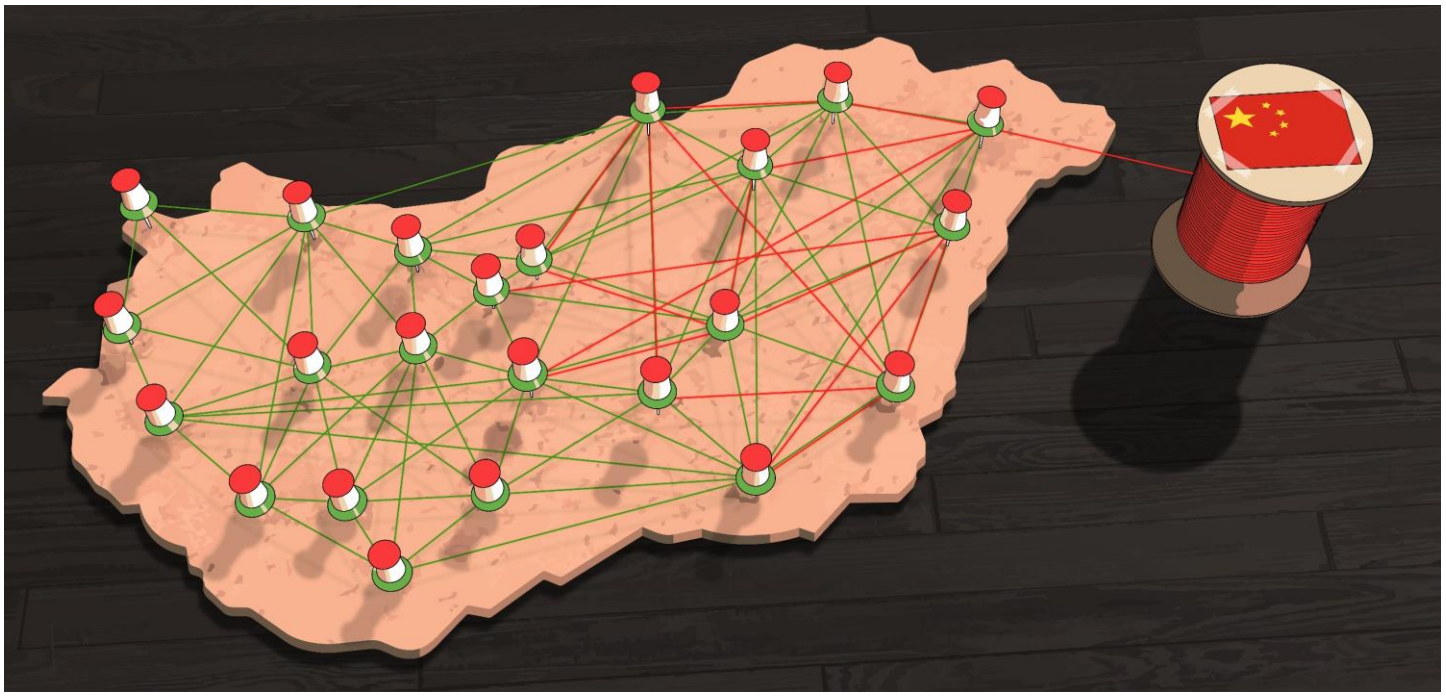


China’s involvement in Hungary’s critical infrastructure

Tünde Lendvai

Dr. András Tóth

A Research Report by the

Central and Eastern European Center for Asian Studies

August 2022

Budapest

EXECUTIVE SUMMARY

- Hungarian national laws consider financial services (banking and credit services), health services and drinking water, energy services (electricity, oil, natural gas, long-distance heating), transport (air, rail, road) and digital infrastructure (telecommunications, internet services, etc.) as critical infrastructure.
- The financial area is influenced by the services of the Bank of China, which is present in five other EU Member States. The overall level of involvement is low, due to the fact that in Hungary there are many alternative commercial banks and credit institutions offering services.
- The involvement of the healthcare sector cannot be measured due to the sensitive and confidential nature of the data.
- The dependency of the energy sector is also low. For the interviewed energy service providers, there are no regulatory requirements that restrict the purchase of software and hardware that can be linked to the PRC. Despite that, experts tend to avoid procurement of Chinese-backed products, which is difficult for network equipment.
- The interviewed energy services sector professionals confirmed that they use IT equipment (mobile phones and laptops) and components (hardware) that can be linked to a Chinese manufacturer to operate critical information infrastructures, but that there is no critical dependency on the supplier.
- In the transport sector, several significant development and logistics projects (Zhengzhou Exclusive Transoceanic Terminal, an air cargo logistics centre) are in progress, depending on Chinese technologies (5G) or investment. The Budapest-Belgrade railway development project has been classified for 10 years in 2021, therefore it is not possible to assess the extent of dependency for this project. However, dependencies on network equipment which are essential for the upgrade of the railway line and Chinese debt financing, should be anticipated.
- Digital infrastructure is highly dependent. Experts in the telecommunications sector have identified 4G and 5G as areas where Chinese solutions may be partially or even entirely affected. Mobile devices that are currently in use by telecom operators in the sector can be replaced at any time, but the replacement of network elements would cause disruption and a significant additional workload for technical staff.
- The technology and expertise that is essential to build certain components of the 5G network in Hungary is currently only available from a Chinese (ZTE or Huawei) or Korean (Samsung) supplier. Therefore, in advance of planning, the technological aspects should be examined of that, whether standardisation or other control solutions can overcome the raised security concerns.
- Given the opportunities for growth of the Hungarian economy and its role in the European market, the chances of the government excluding or restricting Chinese-backed investments and businesses from participating in the development of digital infrastructure are low.

1. Overview of critical infrastructure elements in Hungary

According to the Act CLXVI of 2012, Hungary considers energy (electricity, petroleum, natural gas, district heating), transport (air, rail, road), drinking water (public drinking water), health services (pharmaceuticals and health services), financial services (banking and credit services) and digital infrastructure (telecommunications, internet services, etc.) as critical infrastructure elements.[1] The critical information infrastructure elements which serves at (networks, SCADA, computer systems etc.) these areas are considered essential for daily life. The temporary loss or total failure of critical infrastructure systems can cause significant economic damage and, indirectly, human loss.[2] The paper mainly focuses on critical information infrastructure elements and digital dependences. For simplicity, the author refers to them as critical infrastructure.

The operation of critical infrastructure elements is interdependent (e.g. electricity supply and health services) and the services they provide are interconnected because of cross-border reserves. Therefore, both the European Union (EU) and North Atlantic Treaty Organization (NATO) have developed programs to ensure their systemic protection and to increase their resilience. The success of these programs lies not only in international information sharing and protection exercises, but also in the cooperation of public and private sector maintainers who operate and service these critical infrastructures. Therefore, critical infrastructure elements and their supply and supply chains are also exposed to hybrid and cyberspace threats.[3]

In Hungary, several state bodies are responsible for the protection of critical infrastructure electronic networks in their respective fields, such as the Directorate for Disaster Management of the Ministry of Interior, the Military National Security Service, the National

[1] Government Decree No 65/2013 (8.III.) on the implementation of Act CLXVI of 2012 on the Identification, Designation and Protection of Critical Systems and Facilities Annex 3: List of essential services

[2] Kovács, László (2007): Critical Information Infrastructures in Hungary (Kritikus információs infrastruktúrák Magyarországon), Hadmérnök, Special issue: Robothadviselés 7th Scientific Professional Conference. Available: http://www.hadmernok.hu/kulonszamok/robothadviseles7/kovacs_rw7.html

[3] Fiott, Daniel and Parkes, Roderick (2019): Nuts and Bolts- Safeguarding the critical infrastructure of the Union, EU Institute for Security Studies, Belgium, Bietlot. pp 23-33. Available: https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_151.pdf DOI 10.2815/712409

Cyber Security Center and the National Infocommunication Services Ltd.[4] Foreign involvement in critical infrastructure systems can be manifested in the use of network and physical assets (e.g. laptops, smartphones, cables, software, microchips), telecommunication services (cloud hosting or internet services, 4G and 5G services), in the implementation of development and investment projects, and even in the composition of the investor and ownership base. The research report examines the presence of digital technologies in critical infrastructure that can be linked to the People's Republic of China (hereafter referred as China or PRC), with a particular focus on 5G technology.

1.1 Challenges arising from changes in the regulatory environment for critical infrastructure

Utilizing the potential of quantum computing in offensive cyberspace operations is one of the main directions of modern military technology development. Specifically, the use of analytical capabilities combined with artificial intelligence (AI) in strategic and operational planning. In response to the development of quantum cryptography solutions and protocols announced in the US and NATO Science for Peace and Security (NATO SPS) program, the PRC has also published as one of its development goals up to 2035 the quantum technology capabilities.[5] In parallel, China has allocated significant financial resources to dual-use research on AI and quantum computing. The traditional cryptographic algorithms used today will be made relatively less time-consuming to crack in the future by the proliferation of quantum-based attack methods with extremely high computational power.[6]

Hungarian legislators were the first in Europe to address this potential threat in the amendment to Act L of 2013 on the Electronic Information Security of State and Local

[4] Bonnyai, Tünde: Kritikus információs infrastruktúra védelem, In: Kritikus információs infrastruktúrák védelme (edited by Veronika, Deák) National University of Public Service; Hungary; Budapest. (2019), 231 p. ISBN: 9789634982401

[5] Hungarian National Cyber Security Center (2019); NATO to invest in quantum cryptography (Kvantumkriptográfiai fejlesztésekbe fog a NATO). Available: https://nki.gov.hu/it-biztonsag/hirek/kvantumkriptografiai-fejlesztesekbe-fog-a-nato/
and
Hungarian National Cyber Security Center (2019) China's new military technology developments (Kína új haditechnikai fejlesztései). Available: https://nki.gov.hu/it-biztonsag/hirek/kinai-uj-haditechnikai-fejlesztesei/

[6] Valori, Giancarlo Elia (2019) China’s new military technologies, Modern Diplomacy. Available: https://moderndiplomacy.eu/2019/10/01/chinas-new-military-technologies/

Government Bodies (hereinafter the Act). The amendment requires certain public service providers to implement protection solutions against quantum computer attacks, that apply to the entire operational cycle of electronic information systems. Broadly speaking, this means that the encryption solutions used on individual documents or used, for example, in electronic communication channels and information transmission, must be supplemented with additional protection services. In the wording of the Act, this means the mandatory use of a post-quantum encryption application,[7] must be obtained and operated by a state-certified service provider (not posing a threat to national security). The Act's Chapter III/B containing the rules for the use of post-quantum encryption will enter into force on 1 July 2022, giving the organisations concerned a total of six months to prepare for implementation. Public service providers subject to the law include water, electricity and heating suppliers, as well as public service providers in the natural gas supply sector, banks, and credit institutions. This list of providers covers the elements of critical infrastructure.[8]

The interviewed professionals in the concerned sectors, did not comment on the topic, but it is assumed that further detailed rules will be drafted by the legislators, or a government decision will be issued to help in the practical implementation.

2. Overview of Hungarian-Chinese cooperation opportunities in critical infrastructure

Consistent with the 'Eastern Opening' foreign policy, Hungary has signed strategic agreements with eight major Chinese companies, including Huawei, since 2013. While maintaining these agreements, for foreign economic reasons, Hungary seems much more welcoming to deeper technological cooperation with the PRC and Chinese multinational corporations than the rest of the V4 countries. Hungary was the first European country to join the Belt and Road Initiative

[7] In the wording of the amendment to the Act, post-quantum encryption is defined as: encryption that provides a mathematically plausible post-quantum application or solution applied against a quantum computer attack, over and above traditional cryptography, by using communication between two endpoints to create a shared key between the two end-users during data transmission, without the key being known to an unauthorized third party.

[8] Gyömbér, Béla (2021) Post-quantum encryption is introduced in Hungary (Poszt-kvantumtitkosítást vezetnek be Magyarországon), Jogalappal. Available: https://jogalappal.hu/poszt-kvantumtitkositast-vezetnek-be-magyarorszagon/

and

Act CXXXVI of 2021 amending certain energy, transport and related laws (Hungarian Gazette, No. 231 of 17 December 2021)

(BRI, formerly known as One Belt One Road - OBOR), which has a component named 'Digital Silk Road' aimed at developing electronic infrastructure, including the 5G network. The Hungarian government, like Serbia, has not assessed Chinese tech multinationals as a security threat because of their obligation to provide data for the government.[9] Chinese products continue to be included in open public tenders for the Hungarian state administration.[10]

According to the government's official statement, it has not been proven beyond all doubt that Huawei and other manufacturers have installed backdoors in their devices that allow spying, so it did not give in to the boycott request of the US and other allies. In fact, Péter Szijjártó, Minister of Foreign Affairs and Trade, announced in June 2019 that Hungary, together with Deutsche Telekom and Vodafone, would also commission Huawei to develop certain elements of the 5G infrastructure.[11] The relationship with Huawei will be further deepened by the establishment of an R&D centre in Budapest, that was announced in 2020, which would focus on technologies supporting the development of 5G, as well as image processing and artificial intelligence.[12] Also in 2020, Lenovo announced the construction of a new manufacturing plant in Üllő, replacing the capacity of another Flex-operated plant.[13] The plant, which started operations in spring 2021, produces graphical workstations, data centre products and desktops, winning the National Investment Promotion Agency (HIPA) award for "Most Job-Creating Company of the Year".[14]

[9] Szunomár, Ágnes and Lima da Frota Araujo, Carlos Raul (2022): East-Central Europe on the Digital Silk Road? : Possible political economy explanations. Közgazdasági Szemle, 69 (3). pp. 367-388. ISSN 0023-4346 Available: http://www.kszemle.hu/tartalom/cikk.php?id=2038
and
Government of Hungary (2020); Huawei to build new R&D centre in Budapest (A Huawei új kutatás-fejlesztési központot épít Budapesten), MTI. Available: https://kormany.hu/hirek/a-huawei-uj-kutatas-fejlesztesi-kozpontot-epit-budapesten

[10] E.g.: open procurement of 450 Xiaomi Redmi Note 10 Pro or equivalent smartphones for the Ministry of Information and Technology. Available at (in hungarian): https://www.kozbeszerzes.hu/ertesito/2021/0/targy/portal_454/megtekint/portal_22863_2021/

[11] Szakács, Gergely and Than, Krisztina (2019); Hungarian minister opens door to Huawei for 5G network rollout; Reuters. Available: https://www.reuters.com/article/us-hungary-telecoms-huawei-idUSKBN1XF12U

[12] Government of Hungary (2020): Ibid.

[13] Computerworld (2020): Lenovo to build new manufacturing plant in Hungary (Magyarországon épít új gyártóüzemet a Lenovo); Computerworld. Available: https://computerworld.hu/uzlet/magyarorszagon-epit-uj-gyartouzemet-a-lenovo-285035.html

[14] Szász, Péter (2021); Lenovo receives award for job creation (Munkahelyteremtésért kapott díjat a Lenovo), Available: https://www.napi.hu/magyar-vallalatok/munkahelyteremtesert-kapott-dijat-a-lenovo.736311.html

An international political economics research paper published in 2022 examined the background of Hungary's open attitude towards Chinese technological cooperation and investment along with several other factors in the context of Central and Eastern European countries. The first factor comes from the theory of the local version of capitalism,[15] which explains the deeper cooperation with Chinese ICT companies, the support for Huawei's 5G infrastructure construction and the Digital Silk Road initiative.

On this basis, Hungary can be seen as a dependent market economy, which has successfully attracted working capital from Western Europe by Euro-Atlantic integration and its accession to the EU. What makes the Hungarian market attractive, in addition to government policies to encourage foreign investment and manufacturing, is that the European Structural Funds and other support have given the country the opportunity to build a high-quality manufacturing industry, made more valuable by a skilled, cheaper workforce and easy access to Western European markets. For this reason, Hungary's chance to develop its economy is sensitive to the inflow of foreign capital (which the Hungarian Government welcomes from China and its Euro-Atlantic allies as well) and the decisions of investors from multinational companies.[16]

Another related factor is the lessons that can be drawn from the experience of the 2008 global economic crisis. The Hungarian side sees the expansion and deepening of cooperation with China as an opportunity to reduce interdependence with Western European countries, which would reduce the spillover effect of an economic downturn. However, it needs to be stated that Hungary has a much higher share of trade and investment with its Euro-Atlantic partners, despite the steady rise in Chinese trade indicators. The research has proven that Hungary's current level of digital infrastructure development is mostly equivalent to other EU member states in Central and Eastern Europe, so its digital development is not as reliant on China as in the case of Serbia. Hungary's position can be seen as a rather atypical case in that, despite the controversy over security issues, Hungarian foreign economic and foreign policy is open to Chinese digital cooperation initiatives.[17]

[15] Nölke–Vliegenthart [2009] as cited Szunomár et al. (2022): Ibid pp 379.
[16] Szunomár et al. (2022): *Ibid.* pp 376-380.
[17] Szunomár et al. (2022): *Ibid.* pp 380-381.

The exposure of Hungarian critical infrastructure to Chinese suppliers by hardware and ICT services can be further clarified by the Central and Eastern European Center for Asian Studies (CEE CAS) database of Chinese investments in Central and Eastern Europe. In addition to large telecommunications companies (Huawei, ZTE), Comlink Electronics Hungary Kft., a manufacturer of telecommunications, fibre optic and medical device cables with a regional distribution centre, is a relevant player among potential suppliers to the sector (which does not pose a risk in itself). [18]However, there are currently moves towards domestic majority ownership and centralisation in the Hungarian telecoms sector. An example of this is the enterprise business branch of the Invitel Group (which also supplies critical infrastructure elements), was majority-owned by the China-CEE Fund (one of the largest investors in Central and Eastern Europe) from 2017, but by the first quarter of 2022 it became majority-owned by Hungarian investors through 4iG Plc. and Antenna Hungária Zrt.[19]

Based on the above, the following data and assessments can be made for each of the critical infrastructure elements examined (finance, energy, healthcare, transportation, digital infrastructure and logistics).

2.1. Finance

Dependencies typically occur at the service level, but the level of dependency is low. According to the Hungarian Bankers Association, "the bank's mission is to manage the cash flows, savings and special credit needs of individuals, businesses and institutions in Hungary and the surrounding countries, to finance Chinese trade in the region, and to introduce the Chinese yuan into the settlements."[20] The Bank of China is present in several EU Member States, including France, Ireland, Germany, Italy, Luxembourg, and also operates in the UK and Russia.

[18] Matura, Tamás; Szunomár, Ágnes; Konstantinas Andrijauskas; Una Aleksandra Bērziņa-Cerenkova, Andreea Brînză, Rumena Filipova, Ivana Karásková, Liisi Karindi, Ana Krstinovska, Ornela Liperi, Agnieszka McCaleb, Nina Pejič, Anastasya Raditya-Ležaić, Richard Turcsányi and Stefan Vladisavljev. "Chinese Investment in Central and Eastern Europe Data Set" Central and Eastern European Center for Asian Studies, Budapest, 2021.

[19] Invitech (2022); About Invitech Ltd; Available: https://www.invitech.hu/invitechrol

[20] Hungarian Banking Association: our members - Bank of China. Available at: https://www.bankszovetseg.hu/tagreszlet.cshtml?tagId=5&lang=hun

In Hungary, several alternative commercial banks and credit institutions provide services, so the dependency level is considered low.[21]

2.2. Energy

In the energy sector, interviews with experts indicate that there are no regulatory requirements that restrict the purchase of software and hardware that can be linked to the PRC. Therefore, they avoid purchasing such equipment as far as possible. However, this is difficult in many cases, and there may be cases where some level of China-linked equipment is purchased. The purchase and use of mobile phones and laptops is a typical example of the use of China-linked devices, but experts said these are low risk in their case because they can be easily replaced in case of any compromise or security problem.

2.3. Healthcare

No specific conclusions can be drawn for the healthcare sector, as all data in this sector is classified as sensitive data, so no information is publicly available on the devices, systems, or services used in this sector.

2.4. Transportation

In terms of transport, the expansion of the freight capacity of the Budapest-Belgrade railway line is emerging as a project with Chinese influence. The implementation of the project will improve the connectivity of Hungary (and Western Europe) with maritime freight hubs (e.g. Greece-Piraeus) by reducing the transport time and will contribute to the success of the Belt and Road trade infrastructure development projects.[22] On the Hungarian line, the priority is to upgrade the existing 166 km Budapest-Kelebia railway line. The technical objectives are: double track gauge, 160 km/h operating speed, 225 kN axle load, guaranteeing the interoperability required in Europe by means of the European Train Control System (ETCS 2) and new state-of-the-art safety equipment, thus ensuring an even higher level of railway

[21] Chan; Louis: Hungary: Leading the Way in Sino-CEE Co-operation, Pageo, 2019. Available: http://www.geopolitika.hu/en/2019/02/25/hungary-leading-the-way-in-sino-cee-co-operation/#_ftn3
[22] Chan, Louis; *Ibid*. 2019.

safety.[23] According to press reports from the Ministry of Finance, the development project is worth approximately HUF 700 billion, which Hungary is financing under a loan agreement with the PRC (85% of the project amount is financed by a loan).[24] The Budapest-Belgrade railway development project was classified for 10 years in 2021, so it is not possible to assess the extent of dependency.

2.5. Digital infrastructure

Government Digital Infrastructure: no equipment or service providers linked to the PRC are excluded from the procurement tendered by NISZ Ltd.[25]

Digital infrastructure of market players: For the telecom operators interviewed, no regulatory requirements limit the procurement of software and hardware that can be linked to the PRC, but they typically avoid the procurement of products with a Chinese background.

The exceptions for both sectors are mobile phones and laptops, but as in the energy sector, these do not represent a major dependency.

However, the sector is particularly dependent on the LTE networks currently operating in Hungary and the 5G networks under deployment. Huawei Technologies Hungary is currently able to deploy certain elements of the system, more information on which can be found in the next section.

2.6. Logistics

Corridor V (Helsinki corridor: Trieste-Kiev-Moscow), designated by the European Union transport ministers, passes through the region of Záhony. The logistical importance of the zone lies in the fact that it is the junction of the eastern and western railway tracks, making it a stopping point for east-west freight traffic, and as an external border of the EU, it is also a customs centre.[26] Záhony and its surroundings (Záhony, Tuzsér, Komoró, Fényeslitke and

[23] Hungarian State Railways Group: Chinese-Hungarian Railway Nonprofit Ltd. Available: https://www.mavcsoport.hu/bbproject

[24] Ministry of Finance: loan agreement signed for the Budapest-Belgrade railway line. 2021. Available at: https://www.youtube.com/watch?v=qypQf21nPrU

[25] Hungarian Public Procurement Authority: 450 smartphones to support the controlling, Public Procurement Bulletin, 2021. Available: https://www.kozbeszerzes.hu/ertesito/2021/0/targy/portal_454/megtekint/portal_22863_2021/

[26] Chan, Louis; *Ibid,* 2019.

Nyíregyháza) are excellent locations for attracting long-distance transport-related industrial and logistics businesses, due to their proximity to the Ukrainian, Polish, Slovak and Romanian borders, with high population densities. Within a 200km radius of the area are major cities such as Nyíregyháza (Hungary), Lviv (Poland), Kassa (Slovakia), Satu Mare (Romania) and Lubin (Poland). [27]

The commissioning of the East-West Gate intermodal terminal will increase the volume of rail freight traffic from the east, opening new opportunities for the New Silk Road projects between China and Europe, among others. The terminal will be equipped with an industrial 5G private network, allowing for interoperable internal communications, self-driving and remote-controlled container storage and handling. It is envisaged that cranes transferring freight wagons from the wider eastern gauge to the narrower European gauge will be remotely controlled using 5G technology. The investment of the East-West Gate intermodal terminal (Záhony-Komoró-Fényeslitke) is based on private investment of approximately 30 billion HUF and is expected to start its operations in 2022. The logistics centre is being built by a Hungarian-owned company and will be equipped with a 5G industrial network, jointly implemented by Huawei Technologies Hungary and Vodafone Hungary. Accordingly, Chinese dependence on the project can be established.[28]

Another logistics project in the sector is also showing its dependence on China, the BUD Cargo City, a logistics project between Budapest Airport and airport operator Henan Airport Group. The Zhengzhou Exclusive Overseas Terminal, a warehouse hall at Budapest Airport, which serves as the logistics centre for air cargo from China in the BUD Cargo City air cargo handling

[27] Szabó, Norbert: Fényeslitke, Komoró, Záhony area - Intermodal Logistics Centre: land port at the gateway to East and West, ORIENTER, 2016. Available: http://docplayer.hu/3008330-Orienter-fenyeslitke-komoro-zahony-tersege-intermodalis-logisztikai-kozpont-szarazfoldi-kikoto-kelet-es-nyugat-kapujaban.html

[28] Szabó, Ákos: Europe's largest intermodal terminal is already under construction in Szabolcs, 2021. Available: https://magyarepitok.hu/mi-epul/2021/01/mar-epul-europa-legnagyobb-intermodalis-terminalja-szabolcsban and
Anonymous (MEptech_Admin2): Innovative logistics giga-investment on the home stretch, Hungarian Architecture, 2022. Available: https://magyarepitestechnika.hu/index.php/epites-it/celegyenesben-az-innovativ-logisztikai-gigaberuhazas/

complex, was inaugurated in 2021. The parties agreed in 2021, to establish additional logistics centres.[29]

3. Roll-out of 5G network in Hungary

5G is one of the most significant technological innovations of our time, which could bring many changes in many areas of Hungary's digitalisation. In 2017, the Government adopted Government Decision 1456/2017 (19 July 2017) on the 2016 monitoring report of the National Infocommunications Strategy (NIS), on the Digital Wellbeing Program 2.0, i.e. the extension of the Digital Wellbeing Program, the adoption of its Work Plan 2017-2018, and on the further development of digital infrastructure, competences, economy, and public administration. The resolution states that "the Government's goal is to ensure that all citizens and businesses in Hungary are the winners of digitalization, and that Hungary is among the most successful and best performing countries in Europe in the digital transformation". 5G technology provides the basis for this, enabling new, innovative services and business models, while also expanding the capabilities of telecoms services on a large scale. The Digital Agenda for Prosperity 2.0 (hereafter DAP2.0) sets out the strategic foundations for the development of smart cities, contributing to the development of areas such as smart homes, transport, health, media services, law enforcement and disaster management, which will be greatly affected by the widespread deployment of 5G technology. The importance of 5G is also reflected in the National Security Strategy 2020, which states that "5G technology can enable revolutionary developments that can generate significant changes in our society and economy".[30]

In 2017, the 5G Coalition was established in Hungary to carry out the strategic-level organisational tasks of technology deployment and diffusion, with the fundamental aim of making Hungary one of the centres of 5G development in Europe. The Coalition will continue its activities based on European strategies, guidelines, and regulations, considering the principles and requirements of the Hungarian government and DAP2.0. The formation of the

[29] BUD Airport: Agreement signed, Sino-Hungarian Air Silk Road to be established, Chinese logistics base to be built at Budapest Airport, 2021. Available: https://www.bud.hu/budapest_airport/media/hirek/aktualis_sajtokozlemenyek/alairtak_a_megallapodast_letrejon_a_kinai_magyar_legi_selyemut_kinai_logisztikai_bazis_epulhet_a_budapesti_repuloteren.html

[30] Government Decision 1163/2020 (21.IV.) on the National Security Strategy of Hungary

Coalition in 2017 was an ideal time for many reasons. The European Commission published its 5G Action Plan COM/2016/0588 in September 2016. The aim of the plan was to develop a standardised approach that will contribute to the coordinated deployment of 5G infrastructures. This has not only created and continues to create new opportunities for innovation in the communications sector, but also has a major impact on society, as well as on European and national economies and industry. This requires an appropriate level and scope of coordination at both Member State and sectoral level, in which the 5G Coalition has a major role to play for Hungary. In the Commission's view, the key elements of the plan were:

- To adequately align roadmaps and priorities for the coordinated roll-out of 5G networks across all EU Member States, with a view to a pilot roll-out in 2018 and a large-scale commercial roll-out by the end of 2020 at the latest;
- to make the interim spectrum bands needed for 5G available in advance of the 2019 World Radio Communication Conference (WRC-19), add additional bandwidth as soon as possible and develop proposals for the authorisation of 5G spectrum bands beyond 6 GHz;
- to promote early deployment in major urban areas and along major transport routes;
- to initiate multi-stakeholder European trials as a catalyst for translating technological innovation into full-scale business solutions;
- to facilitate the creation of an industry-led venture capital fund to support 5G innovation;
- to bring together key players to promote the development of global standards.[31]

In December 2018, the EU adopted Directive (EU) 2018/1972 of the European Parliament and Council establishing the European Electronic Communications Code. The Directive aims to stimulate competition for 5G infrastructure and networks by ensuring exclusive regulation of electronic communications by competition law. This will ensure that all EU citizens and businesses have access to high-quality, high-capacity networks and thus to the full spectrum

[31] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 5G for Europe: an action plan.

of innovative digital services.[32]In addition, the Directive includes general objectives such as the promotion of network interconnectivity, ensuring that all citizens and businesses in the EU have access to very high-capacity networks. It allows EU citizens to:

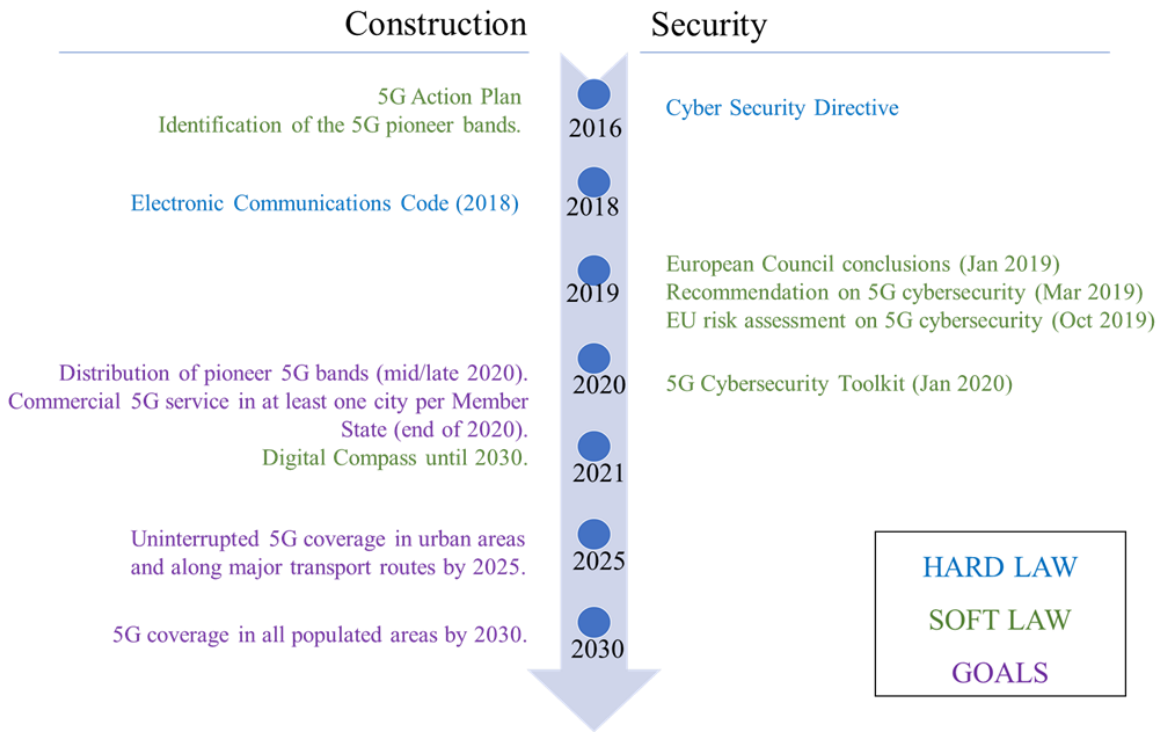
- have the best possible choice, price and quality by ensuring effective competition;
- promote policies to ensure the security of networks and services;
- ensure consumer protection on the basis of the regulatory framework;
- access solutions for all social groups to fully meet their needs (in particular: disabled, elderly and end-users with special social needs).

It foresees the development of common rules and predictable regulation that will contribute to the development of the internal market for EU telecommunications networks and services, ensure efficient and harmonised use of radio spectrum, open innovation, the development of trans-European networks, the availability and interoperability of services across Europe and end-to-end connectivity. In addition, it sets out updated rules covering electronic communications networks, electronic communications services and associated facilities and services, providing guidance to the 5G Coalition.[33] The objectives set out above are illustrated in Figure 1.

[32] Directive 2018/1972 of the European Parliament and of the Council on the establishment of a European Electronic Communications Code.
[33] EUR-Lex: The European Electronic Communications Code

Figure 1.

Main policy documents and key objectives for 5G deployment and security[34]



3.1. The status of 5G infrastructure deployment in the EU and Hungary

The Digital Economy and Society Index (DESI) is a measure of progress towards the key objectives and policy documents to lay the foundations for the operationalisation, deployment, and operation of 5G infrastructures. The first step in the deployment of 5G infrastructure is the allocation of the so-called pioneer frequency bands, which is still ongoing in several Member States and thus across the EU network. Table 1 shows the percentage of harmonised spectrum that was allocated in the 5G pioneer bands for Hungary and the EU.

[34] ECA: Special Report No 03/2022: 5G deployment in the EU: delays in network roll-out, some security issues still unresolved

Table 1.

Percentage of allocated harmonized spectrum

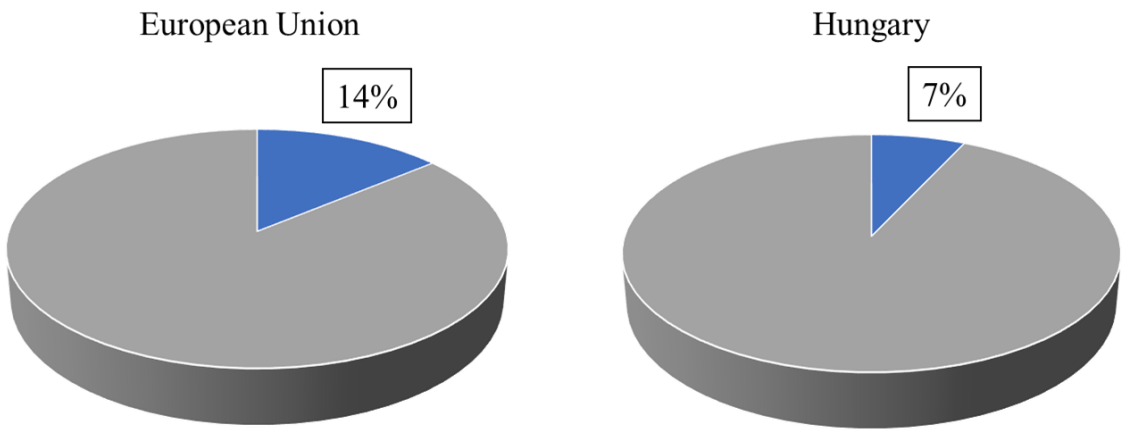
	2019	2020	2021
European Union	14,77%	20,42%	51,42%
Hungary	7,50%	60,28%	60,28%

The above results show that in Hungary the national broadband plans are in line with the 2025 targets, with a high probability of reaching the targets.

After the allocation of the frequency bands, the deployment of 5G infrastructure has started, both in Hungary and in the EU. The process is currently at an early stage. It is expected to provide full coverage in cities by 2025 while national and EU coverage should be achieved by 2030. The percentage of households covered by 2021 is shown in Figure 2.

Figure 2.

Percentage of populated areas covered by 5G



The figure above shows that in both the EU and Hungary, a small percentage of households currently have 5G access. To reach the 2030 target, the 5G Coalition's activities need to be strengthened and expanded, and technological developments need to be accelerated, which

requires the launch of strategic agreements between operators and the government. In addition, the 5G R&D&I support scheme should be continuously developed and Hungary should contribute to the development of 5G corridors in the EU.[35]

The National Digitalization Strategy published in June 2020 provides the appropriate basis and support for this in Hungary, which is based on four pillars, illustrated in Table 2.

Pillar 1	Pillar 2	Pillar 3	Pillar 4
Digital infrastructure	Digital competencies	Digital economy	Digital state
ICT infrastructure for the provision and use of digital services.	Overall digital literacy of the population, digital literacy in the labour market and education.	The broader ICT sector, the related R&D&I, and the external and internal IT systems of businesses using the digital services it provides.	Information and communication technologies supporting the functioning of the state and serving the public, eGovernment, eAdministration services for citizens and businesses, other digital public services of public interest and related information security.

Table 2: Pillar structure of the National Digitalization Strategy[36]

Regarding digital infrastructure, the Strategy sets out the following objectives:

[35] Darijus Valiucko et al.: Study on National Broadband Plans in the EU-27
[36] Ministry of Innovation and Technology:National Digitalization Strategy 2021-2030.

- Achieve 95% coverage of households with a gigabit-capable network by 2030.
- The share of households covered by 5G networks should reach 75% by 2023, covering major transport routes and cities with county status.
- Coverage of district headquarters with National Telecommunications Backbone Network (NTG) endpoints by 2025.
- Achieve 100% coverage of public education institutions with 1 Gbps bandwidth network connections by the end of 2025.
- National HPC (High Performance Computing) capacity to reach 15 Pflops by 2030.[37]

In addition to the above, the Gigabit Hungary Strategy (2020-2030), adopted in September 2019, supports the achievement of all these objectives. Primarily it is to be the first among EU Member States to build an ultra-high bandwidth data transmission network in Hungary, which will contribute significantly to the development of the digital ecosystem. The Strategy sets out the strategic goals and means to achieve the next stage of development of the digital ecosystem, known in the EU as the Gigabit Society, by 2030, along the following pillars:

1. basic infrastructure;
2. network elements;
3. services.

A key priority for infrastructure design is to develop wired solutions that can support next-generation wireless (5G) technologies. These will provide gigabit per-demand transmission links, with symmetrical connections where necessary.[38]

3.2. Chinese dependencies in domestic and EU 5G infrastructure

The first thing to look at in terms of dependency is the technological background. The mobile networks used by 5G can be divided into two main parts, based on functionality and hardware. The first of these is the Radio Access Network (RAN) and the second is the core network. The basic purpose of a RAN is to connect user equipment to other parts of the mobile network by means of radio links, via a network of base stations with transceiver capabilities. The core

[37] Ministry of Innovation and Technology Ibid.
[38] Kormányzati Informatikai Fejlesztési Ügynökség: Gigabit Hungary Stratégia (2020-2030)

network is responsible for those functions that are necessary for the network to function, but do not provide the radio access mentioned above.

Mobile networks can be upgraded to achieve 5G capability in two ways, standalone (SA) and non-standalone (NSA). Non-standalone deployment means that the 5G radio infrastructure is connected to the 4G core network, which creates a significant vendor dependency as in many cases 4G and 5G antennas must work together.[39]

The same problem also applies to 5G security. As networks are deployed and operated by a limited number of vendors, reliance on a single vendor, especially if that vendor is considered high risk, increases exposure to potential supply disruption. This may be the case, for example, in attacks facilitated by suppliers. For 5G, the exposure is significant, especially if the risk factor of each supplier is high. In particular, the likelihood that a supplier from a non-EU country may be subject to some form of external (possibly governmental) interference is a major concern. This may increase the risk by exacerbating the possibility and impact of exploiting weaknesses or vulnerabilities, especially if the dependency involves a high-risk supplier.[40] The main manufacturers and the range of services they provide are shown in Table 3.

Table 3.

The largest manufacturers for 5G[41]

Device manufacturer	Services and solutions	5G infrastructure device manufacturing capability
Huawei	Third generation rugged MIMO[42] solution supporting	Yes

[39] Szőke, Ágoston:Technological characteristics, economic and security implications of 5G and their relation to geopolitics
[40] European Council: report on coordinated EU risk assessment of 5G networks.
[41] European Commission: 5G Observatory Quarterly Report 10
[42] Multiple Input, Multiple Output - technology that uses an extensive antenna system (minimum of two transmitters and two receivers) to generate multiple data streams simultaneously, minimizing signal degradation due to reflections and thus signal delay.

	up to 400 MHz bandwidth (for network sharing). It features a unique, lightweight, integrated passive and active antenna system for easy installation.	
Ericsson	It has developed its own dynamic spectrum sharing service to enable accelerated 5G deployment using existing equipment and systems. The Ericsson radio system will help to rapidly increase 5G coverage, regardless of its size and complexity.	None
Nokia	Nokia works in partnership with several manufacturers. The ReefShark chipset reduces the size, cost and power consumption of individual network elements, while increasing the performance of MIMO antennas.	None
ZTE	It currently has the lightest MIMO solution (22kg), which makes it easy to install in the field and supports 400 MHz	Yes

	bandwidth to support network sharing. Uniquely, it allows dynamic deployment of 3 RAN technologies in the same band (compared to 2 technologies from its competitors).	
Samsung	With extensive experience in time division duplex solutions, Samsung has the capabilities of a robust MIMO radio solution in both C-band and mmWave[43].	Yes
NEC	NEC offers Open RAN-enabled radios, systems integration services enabling the 5G ecosystem, transport networks and telecom cloud, and solutions enabling automation.	None

The table above shows that there is a strong Chinese dependence on the manufacturing of 5G infrastructure equipment. There are several companies developing the technology, but device manufacturing is concentrated in three major companies, two of which are Chinese. This was one of the reasons why in 2015 the EU signed a joint declaration with China on strategic cooperation on 5G, committing to reciprocity and openness in terms of access to research funding and market access for 5G networks. However, following the adoption of China's National Intelligence Law in 2017, the EU reviewed the issue of Chinese suppliers and in 2019 expressed concerns about Chinese 5G vendors who could pose a security risk to the EU due

[43] The 5G high band is the range between 24 GHz and 40 GHz (also known as FR2 - Frequency Range 2).

to their country of origin's legislation. This also raises serious problems with the introduction of the General Data Protection Regulation, as telecoms operators often outsource the data they generate and store to data centres. In the context of 5G, there is a risk that data will be stored by 5G distributors on their equipment in countries outside the EU, which have different legal and data protection levels than the EU.[44] Accordingly, the EU started to squeeze out Chinese suppliers, but Huawei has been the leader in Hungary ever since. The company has made several 5G developments in the country since then, including the launch of Hungary's first 5G industrial service at its own site in 2021. One of the first steps in 5G coverage of major transport routes planned for 2025 is the East-West-Gate (EWG) multi-modal transport terminal to be built near the Ukrainian-Hungarian border, which will combine rail and road container transport. The 5G technology for this will also be provided by Huawei. This shows that Hungary is currently not or only slightly restricting the use of Chinese-backed companies for 5G, which could have an impact on several other critical infrastructures besides telecommunications.

4. Dependences in European critical infrastructure development

Published in 2021, a series of international studies led by Didi Kristen Tatlow and William C. Hannas, examined the volume of scientific and technological cooperation between the EU and China. The research included the elements of critical infrastructure. EU-China scientific cooperation covers joint research on nuclear, aeronautics, agriculture, energy, and environmental issues. The research discovered that, between 2014 and 2020, for example, a total of 464 sub-projects under the Horizon 2020 program involved Chinese experts, funded jointly by the two sides. This figure represents an overall 26% increase in China's share (i.e. Chinese contribution) compared to the EU's share in the previous seven-year funding framework program (2007-2013). Overall, this means that since 2016, the EU and China have invested around €400 million in joint innovation projects, with the EU funding around two thirds and China one third. Based on the results of Tatlow and Hannas, it can be concluded that one of the new analytical factors of Chinese involvement in European critical

[44] ECA: Special Report No 03/2022: 5G deployment in the EU: delays in network roll-out, some security issues still unresolved.

infrastructure projects could be the monitoring of the volume of technology knowledge transfer alongside financial contribution. [45]

Table 4.

Distribution of statements of Central and Eastern European countries on 5G network deployment[46]

Statements of Central and Eastern European countries' on 5G network deployment	
Made no clear decision yet on cooperation with Huawei.	Bulgaria, Northern Macedonia and Lithuania.
The governments stated that they will use Ericsson to develop their 5G infrastructure and not Huawei.	Greece and Croatia.
Have already signed a joint declaration with the US on 5G network security or are ready to join the initiative.	Albania, Czech Republic, Estonia, Poland, Romania, Slovenia, Slovakia, Latvia and Poland.
Reject the suggestion that Chinese companies could pose a security threat. They have stated that they will not exclude Huawei from the 5G network roll-out.	Hungary and Serbia

The table shows that the majority of Central and Eastern European countries reject Chinese digital initiatives and restrict the use of their tools for security and political reasons. Within the V4, this is particularly true for Poland and the Czech Republic, but Slovakia, like Hungary, does not consider Huawei's involvement (e.g. in the construction of transmission towers) as a

[45] Tatlow, Didi Kristen; Hinnerk, Feldwisch-Drentrip; Fedasiuk, Ryan (2021) In: China’s quest for foreign technology: beyond espionage; Europe: a technology transfer mosaic; New York; Routledge.

[46] Szunomár mtsi. (2022); *i.m.* pp 374-376

national security threat in the absence of clear evidence for the deployment of 5G infrastructure. The role of Germany is also noteworthy, as within the region, Latvia, for example, is orienting its position based on Deutsche Telekom's and Vodafone's cooperation with Huawei. Given the interdependence between the CEE region and the German economy, the success of Chinese digital initiatives may be most influenced by the attitude of decision-makers in Berlin and German ICT service providers.[47]

Serbia is considered the second most important partner of China among the Central and Eastern European countries, due to the advantages of Hungary's EU membership, even though most infrastructure development and investment projects have been established here. In terms of critical infrastructure, the Chinese involvement is particularly evident in the implementation of transport investments, but a significant share is also represented by projects aimed at developing digital infrastructure, which is considered to be less developed at regional level. In the latter, the Serbian state telecoms company and Huawei have already started building the telecom backbone for the 5G network.[48] In addition, the Safe City - Safe Society projects in Belgrade are a unique initiative at global level. As of 2019, smart cameras manufactured by Huawei have been installed on the streets, of which at least 1200 have been counted by Serbian activists. Serbian cybersecurity experts and data protection activists have raised concerns about the potential for biometric surveillance, as well as the lack of transparency of the program and the lack of information provided by the government on financial and data management and processing aspects. This latter problem was acknowledged by the Serbian Data Protection Commissioner Milan Marinovic. Responding to this concern, the authorities said that the cameras will monitor car traffic and will play a role in traditional law enforcement and will not be equipped with facial recognition software, as the processing of biometric data is currently prohibited by Serbian law in line with EU accession-related harmonisation.[49] Overall, Serbia has the closest cooperation with China in the development of critical infrastructure, while the diplomacy on the supply of masks and

[47] Szunomár mtsi. (2022); *i.m.* pp 375-376
[48] Szunomár mtsi. (2022); *i.m.* pp 376-379
[49] Gomez, Julian (2021); People worry about the installation of facial recognition cameras in Belgrad (Arcfelismerő kamerák telepítése miatt aggódnak a belgrádiak); EuroNews Available: https://hu.euronews.com/my-europe/2021/07/09/arcfelismero-kamerak-telepitese-miatt-aggodnak-a-belgradiak

vaccines during the coronavirus pandemic has added a new dimension to bilateral political relations (in addition to the status of statehood in Kosovo).

5. Summary of expert interviews

During the research, the author interviewed several professionals working in the field of critical infrastructure. Among the critical infrastructures, it was possible to interview energy and telecommunications companies, and it was possible to interview professionals working in the security field, typically in the field of information security, about the hardware and software capabilities and dependencies of the information infrastructures of their interest.

The questions basically examined whether the IT infrastructure and services of the company in question use Chinese vendors in their systems and networks, whether the use of such software and hardware is subject to additional internal regulation, and whether they have Chinese suppliers in their supply chain.

The first set of questions examined whether there are any regulations in place that restrict the procurement of software and hardware that can be linked to the PRC.

Based on the responses from the energy sector, the result was that there are no such written rules, but they avoid purchasing such equipment as much as they can. However, this is difficult in many cases, and there may be cases where assets are purchased that are to some extent linked to China.

Responses from the telecoms sector also show that they do not currently have regulations prohibiting the purchase of hardware linked to Chinese manufacturers and in many cases do not see any possibility to do so at present.

The second set of questions asked whether IT tools are used in everyday work that can be linked to a Chinese manufacturer at the hardware level, and whether this implies a technological dependency on China.

Based on the answers of the energy sector experts, the result was that both computers, laptops and mobile phones use devices that can be linked to a Chinese manufacturer to some extent. In many cases this is unavoidable, as there are many devices in the market today that

are essentially linked to a US or European manufacturer, but parts or in some cases even the whole device is manufactured and/or assembled in China, typically for economic reasons. When asked whether this creates any dependency, the unanimous answer was that it does not at present. Should a serious problem arise with any of the devices, they could be replaced quite easily.

Telecoms sector specialists also highlighted laptops and mobile phones but there are also network components that are now being linked to Chinese manufacturers. They do not feel a strong dependence on manufacturers for the former, but for network components, the replacement of a network component could be a serious problem. In most cases, this would entail a significant financial cost and a very heavy extra burden on the technical staff.

The next set of questions looked at IT services, typically whether services are used for which a Chinese company could be the sole or dominant supplier.

Such services do not appear in the energy sector, where domestic, European, and American solutions are typically used. Accordingly, the energy sector is not at all affected by Chinese dependence.

However, in the telecoms sector, 4G and 5G were identified as areas where Chinese solutions may be partially or even entirely relevant. Going back to the previous question, they said that Chinese devices used in these networks run Chinese services, which are inescapable, and there is therefore a strong dependency on them.

The final area looked at cyber security, typically whether there had been any recent attacks that indicated Chinese-backed activity.

Responses from both sectors indicated that there was no evidence of an explicit Chinese attack, but it cannot be excluded that a Chinese-linked group may be behind an incident.

6. Summary

The research report found that the following factors can be used to estimate the extent of current and future Chinese involvement in Hungarian critical information infrastructures.

Based on the results of Tatlow and Hannas, it can be concluded that when assessing Chinese involvement in EU CII development projects, it is worthwhile to consider the volume of

technology knowledge transfer and the dependency on the level of funding as a proportion of total R&D&I projects. The results of the cited research by Szunomár and Carlos Raul demonstrate that the Hungarian foreign policy position on the use of Huawei as a 5G infrastructure provider is atypical compared to the position of other Central and Eastern European EU Member States with similar economic structures and digital development. Given the potential for growth of the Hungarian economy and its role in the European market, there is little chance that the government will exclude or limit the participation of Chinese-backed investments and companies in the development of digital infrastructure. However, during the expert interviews, public and private actors operating critical information infrastructure were seeking to avoid non-transparent suppliers, e.g. from Chinese backgrounds, due to information security and privacy concerns. The experts interviewed confirmed that they use IT tools and components that can be linked to a Chinese vendor in the operation of CIIs, but that there is no critical dependency on the supplier. The exception to this is 4G and 5G data transmission technology, where there is a significant dependency.

The full technological and convenience functionality of industry4.0's innovative manufacturing and warehousing solutions, smart city projects and Internet of Things (IoT) devices can be harnessed through 5G data transmission. In the future, solutions based on 5G data transmission will also be used by public and private operators in the energy, healthcare, and financial sectors, as well as in the defence and security fields. Therefore, the deployment and maintenance of 5G networks will be considered as a critical infrastructure element. The technology and expertise to build some components of the 5G network are currently only available from Chinese (ZTE or Huawei) or Korean (Samsung) suppliers (see Table 3). Therefore, from a technological point of view, the possibility of addressing the security concerns raised, either through standardisation or other control solutions, should also be explored. The willingness of multinational telecommunications companies to cooperate in the deployment of 5G networks is also relevant. In the case of Hungary, this may also depend on the attitude of Deutsche Telekom and Vodafone, and more broadly of German industrial and political elites.

The research was supported by the grant of the US Embassy in Budapest as part of a larger project titled 'Risky Business? Assessing Political Economic and Technological Risk Perceptions of Relations between the People's Republic of China and Hungary'. The project examines the relations between Hungary and China in four main areas. In addition to the media relations described in the present research report, the research team also examined the image of China in the Hungarian public, the image of China among the Hungarian political and economic elite, and China's involvement in Hungarian critical infrastructure.